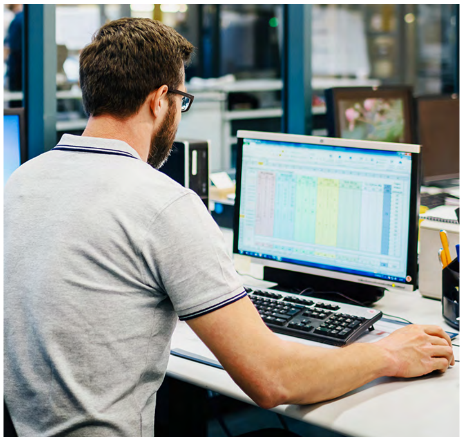
Product Flyer

opentext™



Bring Sanity to Mainframe Access with Automated Sign-On

Albert Einstein said that doing the same thing over and over again—and expecting different results—is the definition of insanity. Similarly, applying the same security to mainframe access year after year and expecting it to magically become more secure is, in fact, insane.

While the security for accessing enterprise applications has evolved to match new security threats, the security for accessing mainframe applications has stayed the same for decades. This stagnation has occurred for three key reasons:

- First, legacy mainframe applications still do the heavy lifting in most businesses. Changing them is risky, difficult, and expensive. Even finding the human resources to update the security access controls for these apps is nearly impossible.
- Second, large enterprises often lack the internal will to dive into the mainframe "can of worms." The IT dialogue goes something like this: What if we break something? What if it's much more complicated than we thought? What if our business goes down? We can't pull the mainframe into a safe harbor and fix everything while we are running our business. Plus, the costs to duplicate that environment are too high in terms of time and money.
- Third, there's a perception that the mainframe is safe and secure behind the firewall—that only authorized users can get into it. But there's no guarantee that a malicious someone won't steal or hack into someone else's mainframe logon credentials. Those older apps use weak eight-character, case-insensitive passwords. There isn't a network admin on the planet who thinks those passwords are strong enough to protect anything—especially intellectual and customer information.

The question is, how do you break a pattern of insanity when some of the reasons for the behavior are based on very real and logical fears?

The Mismatched Security Systems of the Enterprise

Within most enterprises there are two security systems. One is the Identity and Access Management (IAM) system used to provide access to enterprise resources and applications. IAM systems require the use of a strong password to gain access—typically one with a minimum of 12 characters, including upper and lower case letters, numbers, and special characters. Strong passwords are infinitely more difficult to hack or steal.

Mainframe systems also have their own form of "IAM," typically known as RACF or Top-Secret. These systems provide authentication and authorization to mainframe resources. The problems is that, by original design, the applications that use these systems require only weak eight-character passwords.

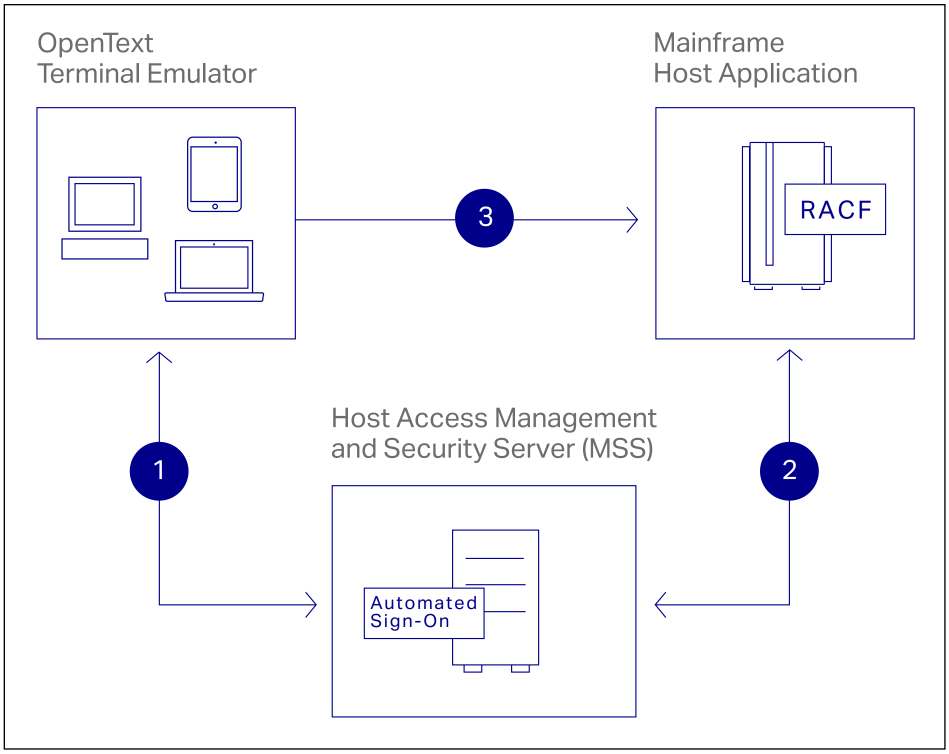
So we have two separate systems providing access to enterprise resources. And one has to ask: Why is it okay to require strong authentication for accessing enterprise applications but only weak authentication for accessing mission-critical mainframe applications, the ones that run your business? That's insane.

End the Insanity

What if there were a way to use your IAM system to control and manage access to your host system? In fact, there is. It's called OpenText™ Host Access Management and Security Server (MSS).

MSS finally brings sanity to the enterprise by integrating your mainframe with your existing Identity and Access Management (IAM) system. MSS puts a security control point between users that need mainframe access and your host systems. It uses your existing IAM structure—specifically, strong authentication—to authorize access to the mainframe.

MSS also provides an add-on product—Automated Sign-On for Mainframe—to take sanity to new level. Automated Sign-On for Mainframe enables automatic sign-on all the way to the mainframe application—eliminating the need for users to enter any IDs or passwords. Imagine that. No more mainframe passwords.



1. The emulator launches a session and requests user credentials for the host application from Automated Sign-On.
2. Automated Sign-On requests a one-time-use PassTicket from RACF and sends it back to the emulator.
3. The emulator uses a one-time-use PassTicket credential to automatically log the user on to the host application.

Other MSS add-on products provide additional critical security for host access:

- **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 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.

MSS and these add-ons leverage your existing resources and infrastructure so can use what you already have in place to secure and manage host access. They deliver sustained business value while driving lower TCO. In these ways, they also bring sanity back to enterprise security.

Learn more at
www.opentext.com

Connect with Us

opentext™