SOLUTION BRIEF
MAINFRAME SECURITY MANAGEMENT

How Can Advanced Authentication Mainframe features from CA Technologies Enhance My Enterprise Security in the Application Economy?

Advanced Authentication Mainframe features create a consistent, multifactor authentication approach to prevent data breaches and address customer compliance requirements.

Executive Summary

Challenge

Mainframe systems store 80 percent of corporate data in industries such as financial services, healthcare, transportation and telecommunications.[1] Not only is this data critical to operations but it can also be sensitive, regulated for privacy—and its disclosure can cause significant financial ramifications and reputational damage. With the mainframe's interconnectedness in the application economy, securing access to mainframe applications with only a password is no longer secure enough.

Opportunity

Advanced Authentication Mainframe can significantly increase the security of application access. By requiring additional information beyond a password, applications have greater assurance that its users are who they say they are. Working with External Security Managers (ESMs), CA ACF2™, CA Top Secret® and IBM® RACF®, Advanced Authentication Mainframe features deliver multifactor authentication to strictly control who has access to critical business resources.

Benefits

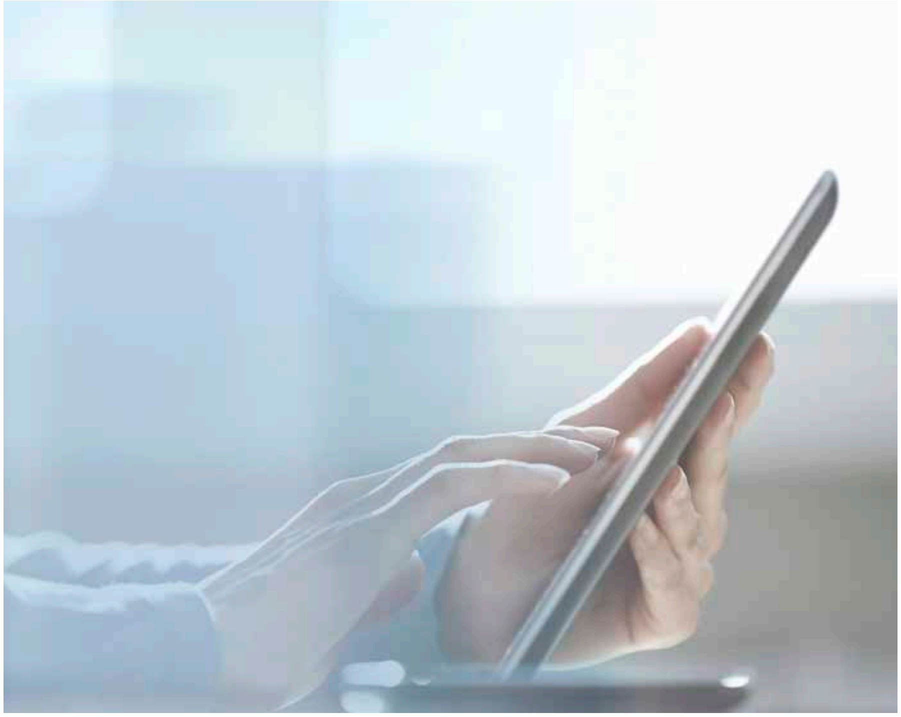
Advanced Authentication Mainframe is designed to help you address compliance mandates and leverage the same authentication mechanisms as enterprise systems, while remaining implicitly mainframe ESM-centric. Now included in ESMs, CA ACF2 and CA Top Secret—at no additional cost to licensed customers—Advanced Authentication Mainframe features address NIST requirements and support hard and soft tokens for two-factor authentication to the mainframe, providing the extra layer of security needed to protect against the rising tide of social engineering attacks.

Section 1:

When It Comes to Security, There Are No Excuses

Insufficient or loose access controls for privileged users are consistently the top cause of major security breaches. In the application economy, the mainframe is no longer locked down. Increasingly vulnerable to attack, this crucial, high-speed and completely reliable transaction processing backbone is pervasively interconnected with other servers in the infrastructure as well as with the external Internet. Which means today's modern data center demands additional layers of security to protect your businesses' mission-critical data. Insider threats, social engineering, retiring mainframe experts and skill gaps combine to create the perfect storm where unintentional negligence can leave critical data and resources exposed.

Advanced Authentication Mainframe provides the additional layers of defense in depth that are now a must across mainframe and enterprise systems. It updates security controls to needed levels of durability and mitigates the risk of data breaches—all while addressing compliance mandates to provide you with unified, multifactor enterprise security and peace of mind.



Gain unified enterprise security and peace of mind.

Section 2:

You Can't Secure Mainframe Applications With Just a Password Anymore

In the application economy, the mainframe hosts the majority of the world's mission-critical data. Not only is this data crucial to the operations of most of the world's largest companies but its disclosure can cause significant financial consequences and reputational damage.

Access to mainframe data is often enabled by applications that are secured by a standard user ID and password limited to eight characters. While this was once a reasonably secure method of authenticating a user, with today's sophisticated threats, that's no longer the case. Hackers have been successful in executing dictionary attacks and discovering passwords in a matter of hours.

Increasing the Security of Application Access

The main reason why it's easy for hackers to discover passwords is because users typically choose memorable ones. Even when forced to introduce numbers and special characters, users still have the tendency to create character strings that look like real words. Attackers know this pattern and exploit it. Securing mainframe applications with only a single layer of authentication no longer protects against threats when hackers are continually trying to get in.

The Need for Multifactor Authentication on the Mainframe

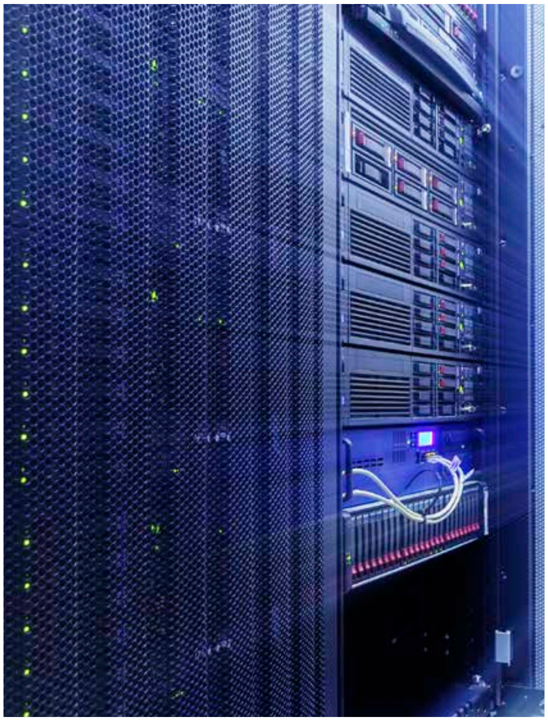
Mainframe application owners are concerned about evolving threats of illicit access. Data custodians are worried about the growing vulnerability of the increasingly large stores of regulated data. Mainframe security administrators want to ensure the proper access controls are in place. And CISOs need to safeguard the corporation.

In the application economy, securing mainframe applications with only a password is no longer secure enough.

Data breaches on the mainframe have occurred, not due to the mainframe itself, but to weak passwords created by privileged users with elevated access. As with any other platform, mainframe security requirements need to be constantly evaluated. Mainframe-proficient staff are retiring, and leading mainframe shops realize that a lack of understanding, training and investment can lead to undesirable—even catastrophic—consequences.

Moving past application access, the mainframe has been collecting data for more than 50 years; locating regulated or sensitive data on the mainframe is time consuming and often impossible. In order to secure files, databases and critical data warehouses, organizations need additional layers of defense-in-depth security protection.

Advanced Authentication Mainframe addresses these needs and significantly increases the security of mainframe application access. By requiring additional information beyond a password, applications have greater assurance that users are who they say they are, which helps enhance your enterprise security.



Advanced Authentication Mainframe significantly increases the security of mainframe applications.

Section 3:

Advanced Authentication Mainframe Key Features

To provide a consistent multifactor authentication approach across the enterprise, Advanced Authentication Mainframe, integrated with RSA® SecurID®, is included in CA Top Secret and CA ACF2 at no additional cost to licensed customers.

Advanced Authentication Mainframe is designed to prevent data breaches and address customer compliance requirements by leveraging the current security infrastructure; automatically mapping user IDs; delivering compliant, two-factor authentication for privileged or all users on the mainframe; automatically updating controls; and addressing National Institute of Standards and Technology (NIST) requirements for two-factor authentication.

Specifically, Advanced Authentication Mainframe

- Addresses compliance mandates, including NIST requirements and supporting hard and soft tokens for two-factor authentication to the mainframe
- Uses the current security infrastructure by leveraging CA Top Secret and CA ACF2 R15 or 16 installations, along with current RSA SecurID v7.x or v8.x infrastructure for implementation
- Provides identical authentication process as enterprise systems by enabling a consistent, two-factor authentication approach across mainframe and enterprise infrastructures (for those organizations using RSA SecurID)
- Secures privileged or all users by requiring any individual user, group of users or all users to successfully authenticate with two factors before logging in to mainframe applications
- Maps IDs, which chart user IDs between the mainframe and RSA Server
- Enables flexible implementation by requiring selected applications to use two-factor authentication and by leveraging all authentication options offered through RSA SecurID

Section 4:

Conclusion

The application economy directly influences IT trends for how existing investments in mainframe systems should be managed. As the number one independent software vendor (ISV) based on revenue for mainframe software and the number two software vendor based on revenue for IT operations management software[2], CA Technologies continues its investment in mainframe data protection offerings. Mainframe Security Management from CA mitigates the risk of data exposure, reduces the effort associated with regulatory compliance and maintains a unified enterprise security 100 percent on the mainframe to keep your mission-critical corporate data secure.

[1] Computer Weekly, “Can the mainframe Remain Relevant in the Cloud and Mobile Era?” March 2014

[2] Gartner, “Market Share Analysis: IT Operations Management Software, Worldwide, 2014,” May 2015

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein.