EXECUTIVE BRIEF | APRIL 2016

CA Advanced Authentication

Why You Should Upgrade to the Latest Release?

Shorten the time to upgrade with a new upgrade tool from CA.

CA Advanced Authentication is a packaged solution that combines two leading authentication solutions:

- **CA Strong Authentication** (formerly CA AuthMinder/WebFort) allows you to deploy and enforce a wide range of strong authentication methods in an efficient and centralized manner.
- **CA Risk Authentication** (formerly CA RiskMinder/RiskFort) offers your organization the ability to detect and block fraud in real time based on contextual risk analysis and user behavioral profiling.

One of the most time-consuming tasks associated with any upgrade is migrating the application databases to a newer version. The new CA Advanced Authentication upgrade tool can significantly reduce this effort—helping you reduce weeks of tedious work to days. Based on your implementation decisions, this could happen without any outage or downtime. The tool also allows you to trim the data stored in the database (for example, to transfer only a few months of recent data). While this is configurable, best practices have shown that only the past 90 days of authentication history data is most relevant in most environments.

Customers running WebFort 6.2.x or 7.1.x and/or RiskFort 2.2.x or 3.1.x can use the new tool to upgrade to the latest release of CA Advanced Authentication (8.1.3), which includes many new features and product enhancements (described in the following tables). In addition to the enhancements, the tool can help you migrate off platforms (application server, database server and OS) that are no longer supported by their native vendors. You'll also benefit from a number of defects fixes that have been added since your current version was released.

What's new about CA Strong Authentication?

Solution	New Capability	Description
CA Strong Authentication	Credential enhancements	The solution now supports warning and grace periods for all other credentials, can issue multiples of other credential types (besides passwords), and can maintain a history of CA Auth ID passwords and admin passwords to enforce password-reuse rules. A new token management page allows you to bulk load OATH tokens (you can also do this via a bulk-upload web service).
	CA Mobile OTP enhancements	The solution supports OATH and EMV-based OTPs as well as roaming for OATH-based or EMV-based CA Mobile OTP. Now, admins can perform synchronization for time-based and counter-based OTPs for the end user. We also introduced CA Mobile OTP client for the PC.
	Integration enhancements	The solution provides software development kits (SDKs) for the CA Auth ID and CA Mobile OTP, which allow customers to build custom clients for these credentials. Libraries are also included that allow these credentials to be embedded into mobile apps.
	Security enhancements	The solution applies salt-based encryption to most user, credential and configuration parameters, as well as supports authentication and authorization for all web-service calls.
	Unbreachable password	The solution introduces a new use case for the CA Auth ID credential called unbreachable password. Using this approach, customers can eliminate storing passwords in backend repositories.

What’s new to CA Risk Authentication?

Solution	New Capability	Description
CA Strong Authentication	Configurable rules engine	The solution provides a simplified user interface for managing rule and lets you can add custom rules and/or actions within the rule-builder interface.
	New rules	In addition to offering the capability to combine rules, the solution introduces several new rules, including: ▪ **Action Velocity**, which limits the number of specific actions by a user over a specified time interval ▪ **Device User Velocity**, which allows a device to be used by “n” distinct users in any configured duration ▪ **Device User Maturity**, which enables a level of trust in the device-based device association history and the number of successful transactions with that device
	Mobile channel	The solution can collect unique data that is available on mobile devices, which is used to fingerprint the device. To collect this data, the solution provides Mobile SDK libraries that are embedded into mobile apps.
	User behavior profiling	This functionality measures the similarity or difference of the current user transaction with prior history by the same user to determine if the transaction falls within or deviates from a normal pattern.
	Interface enhancements	The solution now provides return response and reason codes, as well as a Representational State Transfer (REST) interface for risk assessment.
	Administration enhancements	The solution now provides a comprehensive screen that allows you to manage Risk Authentication server instances. By introducing improved audit log data management, you can now trim the audit log data and move it to backup tables using an automated process. A new report download tool makes it easier to access the data you need.

r

Previously, CA Advanced Authentication supported out-of-band one-time password (OTP) functionality across mobile, voice and email channels as a custom integration with a third-party service provider. Now, CA provides the ability to integrate directly with our internal hosted messaging service, creating an easier onboarding option for CA Strong Authentication and CA Risk Authentication customers that can be enabled without any customization.

For more information,
please visit http://www.ca.com/us/products/ca-advanced-authentication.html

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.