SOLUTION BRIEF
CA ADVANCED AUTHENTICATION

How can I provide effective authentication for employees in a convenient and cost-effective manner?

ca technologies

CA Advanced Authentication provides a flexible set of easy-to-use, multi-factor credentials and transparent, risk-based evaluations to improve the security of corporate applications and data and protect your employees' identities.

Executive Summary

Challenge

In this mobile world, information, applications and users no longer stay inside the enterprise but work from wherever the business needs them. Security must exist in this world of disappearing perimeters. Organizations must both embrace and secure the open enterprise. Unfortunately passwords are often a critical weak link in a web-based security system, and they fail to satisfy many industry best practices and regulatory guidelines for protecting identities and data. Today's approach of relying solely on a credential to validate user identity has shown to be vulnerable to attacks. Organizations need a more secure way to protect access to corporate applications and data and protect their users from account takeover.

Opportunity

CA Advanced Authentication provides a secure, user-convenient and cost-effective way to protect many sensitive corporate resources, including cloud-based services, privileged accounts, remote access, virtual desktops and Web resources. CA Strong Authentication provides a wide variety of software-based, multi-factor authentication credentials and CA Risk Authentication provides real-time, transparent risk evaluation based on user behavior, device characteristics and geolocation data. Together they enable an intelligent, layered security approach to protect user identities and organizational data.

Benefits

Verifying the identity of a user before granting access to sensitive information reduces the risk of inappropriate access. It provides additional security for all the applications and confidential data that can be accessed through a browser or mobile device and thus helps reduce the risk of employee identity theft, corporate espionage, intellectual property theft and other data breaches. Providing this protection in a familiar, user-friendly manner allows organizations to improve security and reduce fraudulent activity without impeding the productivity of employees or partners.

Section 1:

Securely connect employees, contractors and partners with business applications.

As enterprises seek to achieve greater revenue and efficiencies from e-business and mobility channels, the degree of information security risk increases. With the growth in users, applications, devices and access channels comes an inevitable increase in the amount and types of sensitive data that they access. This typically spans a spectrum from personally identifiable information about employees that must be handled carefully, to a wide range of enterprise data that needs to be protected from inappropriate access. Much of this sensitive information is protected by internal security policies, privacy guidelines or regulatory compliance, but each new application potentially brings a new and different way to access confidential, proprietary, or regulated data. A critical success factor for enterprises conducting business over these new channels is the ability to authenticate and authorize users in a unified, consistent, convenient and cost-effective way.

Often there is nothing more than a simple username and password protecting access to applications. When used as the only form of authentication, passwords can be a weak link in security. Recent attacks, such as phishing, man-in-the-middle (MITM), brute force, spyware and social engineering, show how easily passwords can be compromised. And once login credentials have been compromised, attackers can gain easy access to the organizations internal network and the wealth of valuable information it contains. To reduce this risk, most security experts recommend the replacement of simple username/password combinations with stronger authentication and several regulations recommend, or require, multi-factor authentication. Factors can include the following:

- Something you know (such as password or PIN)
- Something you have (such as smartcard, digital ID or one time passcode generator or mobile device)
- Something you are (a biometric factor such as fingerprint or voiceprint or user behavior)

The challenge is to adequately verify user identity before providing access and to give organizations the confidence to make increasingly sensitive information and activities available to employees, contractors and business partners. This has to be done in a way that is user-friendly and convenient to promote adoption and preserve the original goals of efficiency and employee productivity. This also needs to cover the following critical areas: VPN remote access, single sign-on to intranet and extranet portals, cloud-based services, privileged users, virtual desktop infrastructure (VDI) and mobile devices.

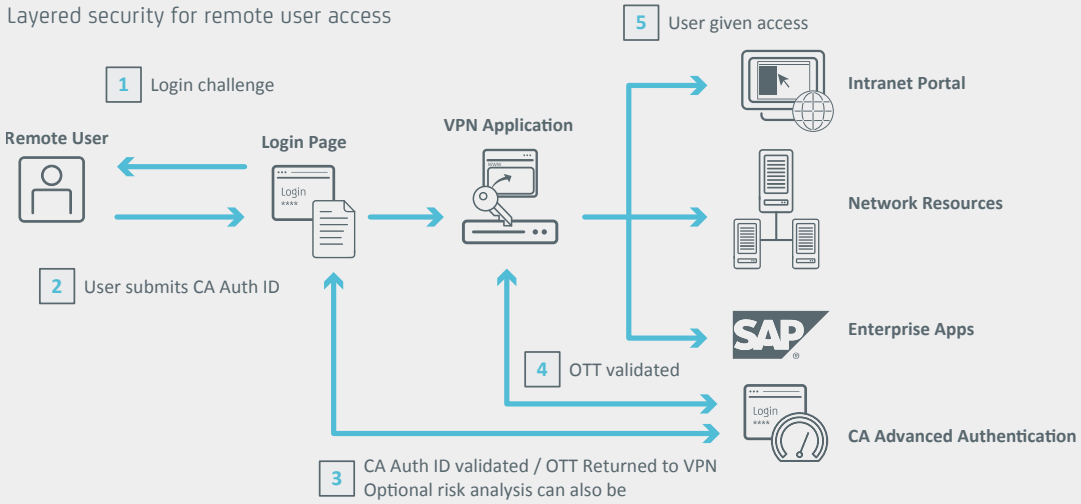
Remote access is vital to business today.

Today's business environment demands strong communication and quick turn-around times. Employees, contractors and business partners want access to the information they need, where and when they need it. In the past ten years, organizations have consistently added data and applications to employee and partner portals that are protected by VPNs. In most instances, users can access confidential product information, non-public financial data, organizational/personnel information, benefits and healthcare information, personal financial information and more through the VPN. And although VPNs create a private "tunnel" that helps keep the information that flows through it private, they do not prevent unauthorized access to the organization's network. Often a simple password is protecting the "first mile" of a VPN. Historically VPNs were one of the first technologies to incorporate hardware-based OTP tokens for stronger authentication for remote users. Unfortunately this approach proved to be too expensive and impractical for larger user communities and cumbersome for end users. Organizations are turning to software-based solutions that are user-friendly, convenient and less expensive.

Figure 1.

One of the primary use cases that led organizations to purchase and deploy CA Advanced Authentication is to address remote users accessing their network. In this case, the solution is generally integrated with their SSL VPN appliance to support strong authentication at initial VPN login.

CA Advanced Authentication integration with VPN appliances



CA Advanced Authentication addresses this use case through the issuance of a software-based, multi-factor PKI credential (CA Auth ID) and risk analysis. When users navigate to the VPN login URL, they are redirected to the CA Advanced Authentication login page. This page issues the hidden PKI challenge to the user's CA Auth ID and also collects the data necessary for the risk evaluation, if required. The user is prompted to enter their user ID and password. The password is used to decrypt the private key, which signs the challenge. The user ID, signed challenge and risk data are then forwarded to the server for validation and evaluation. Assuming that these checks are successful, the server generates a one-time token (OTT), which is forwarded to the VPN appliance along with the user ID as header variables. The VPN appliance validates the OTT over RADIUS and authenticates the user to network resources and any corporate portals or applications that are also accessible after a network login.

Single Sign-On (SSO) does not necessarily need to be single credential.

Organizations must rapidly respond to business opportunities with the ability to develop and deploy new Web applications while IT budgets are flat or decreased. They must also address:

- **Poor user experience accessing Web and cloud applications**–Maintaining separate sets of credentials for each application or authenticating for every access to an application can be frustrating.
- **Rapid increase of new applications, especially mo**–Organizations are looking to quickly deploy new applications to grow their business.

SSO solutions address these business challenges. However, not all applications are created equally; some applications provide access to critical data and therefore require stronger authentication mechanisms. This requires that organizations implement authentication strategies based on the type of data or application being accessed, and not just during initial authentication, but continuously throughout the session. Because user sessions can be stolen it is essential to employ risk analysis within the session to prevent cookie replay attacks.

CA Advanced Authentication addresses this use case through several out-of-the-box adapters that allow the solution to be easily and quickly integrated with leading Web access management/SSO solutions, including CA Single Sign-On (CA SSO), IBM Tivoli® Access Manager and Oracle Access Manager. If one of these solutions is present, then the adapter could be installed and configured to allow these systems to protect Web applications and resources with risk evaluation and multi-factor authentication credentials. If an SSO solution is not being used to protect the intranet or extranet portals, CA Advanced Authentication provides both SOAP-based Web service APIs and a Java™-based SDK (which can be embedded in an application or login page) that allows these to collect multi-factor credentials and/or risk analysis data and forward to the solution servers for validation and evaluation.

In addition, the CA Advanced Authentication risk analysis engine has been embedded within CA SSO to provide enhanced session assurance with DeviceDNA™. This capability helps prevent unauthorized users from hijacking legitimate sessions with stolen cookies. When the user is initially authenticated, CA SSO collects specific data from the client machine and uses our patented DeviceDNA™ process to fingerprint the device. This fingerprint is stored in the session cookie and it is validated on each new request. This validation assures that the client who initiated the session is the same client who is requesting access, which prevents unauthorized users from hijacking legitimate sessions with stolen cookies. This is a powerful combination of benefits, any one of which could be used to justify the solution, but together create a compelling business case for any organization.

To cloud or not to cloud—don't let security cloud your decision.

Organizations are leveraging cloud-based services across all areas of the business in order to increase the speed with which they can deploy and scale applications while simultaneously reducing operational cost and risk. However regulatory and compliance controls apply to all infrastructure and software operations, irrespective of whether they are deployed on-premises or via SaaS. Therefore organizations need to safeguard any sensitive or confidential data that may be stored or processed in the cloud. While the cloud service providers bear the responsibility for data center security, both physical and logical passwords are the most commonly used methods to authenticate to these services and are once again the weak link in the overall security of the service.

SSO and federation technologies can be used to minimize this risk by integrating the cloud services with an organization's intranet, allowing internal users to federate into the service without entering any credentials. However, most cloud services also allow users to login directly to the service when they are off network. Remote users will often access these applications directly as it is more convenient and, in some cases, much faster than logging into the corporate network first. Incorporating risk-based and two-factor authentication with this direct login scenario will mitigate the risk.

CA Advanced Authentication addresses this use case by easily integrating with cloud-based applications via standards-based federation protocols. The most common approach is to configure the cloud application to redirect the user along with a SAML 2.0 request to a login URL protected by CA Advanced Authentication. The solution will authenticate the user, generate a SAML assertion and redirect the user back to the target application. CA Advanced Authentication can also be integrated with cloud-based services that support WS-Federation/ADFS.

Reigning in the Kings of the Kingdom—Privileged Users

Privileged identity management (PIM) lies at the core of any program to reduce insider threats. Privileged accounts have the access needed to view and steal sensitive information, as well as to cause damage to an organization's network. But the risks associated with privileged identities go beyond insiders. When attackers breach a network perimeter as part of a targeted cyber-attack or advanced persistent threat, they nearly always seek to gain access to privileged accounts to access sensitive data, to install software such as rootkits and backdoors and to cover their tracks. Unauthorized access to critical servers can wreak havoc with reputation and brand equity, as well as potentially leaving the organization at risk of significant liability.

A common starting point that organizations deploy to reduce the threats posed by their privileged accounts is to control passwords, which is frequently called shared account management or privileged user password management. While important, this approach fails to sufficiently reduce the risks posed by privileged accounts because the mechanism used to authenticate users to check out the password for a privilege account is another password. Incorporating risk-based and two-factor authentication with a PIM solution will significantly enhance the security of these privileged accounts.

CA Advanced Authentication has been integrated with CA Privileged Identity Manager. Users requesting a password for a privileged or shared account can now be required to authenticate with the CA Advanced Authentication multi-factor authentication credentials and risk evaluation. This helps protect your most sensitive identities from breaches by both malicious insiders and external attackers through the use of two-factor authentication.

Enabling the Mobile Device

Users are increasingly turning to mobile apps as their preferred access channel and this is true across all types of interactions--consumers to business, citizens to government, business to business and, especially, employee to employer. The business can realize significant savings and productivity gains by allowing is employees to access corporate resources via mobile devices; however securing access from these mobile apps to sensitive corporate data is extremely difficult as standard passwords with complex composition are not user friendly. Incorporating advanced authentication within the app itself will address this weakness.

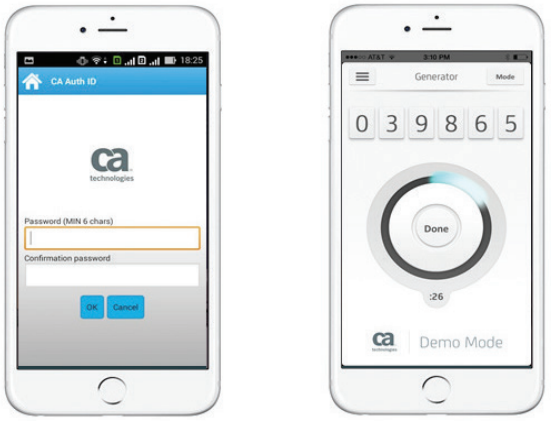
> “ Adopting significantly different authentication methods for different devices will eventually be unsustainable. Mobile authentication methods must also be PC [compatible]. Combinations of X.509 credentials on the endpoint, low-friction biometric modes and contextual authentication will likely fit the bill.”[1]

CA Advanced Authentication provides a CA Auth ID app and a CA Mobile OTP app for most smartphones and tablets, including Android, Blackberry, iOS and Windows® Mobile. These apps can be downloaded for free from the respective app store. In addition the solution also provides libraries for Android and iOS so organizations can develop their own mobile clients or embed the multi-factor credentials and risk data collectors into homegrown mobile apps. CA Advanced Authentication also supports browsers running on the mobile device through a pure JavaScript client.

The CA Advanced Authentication multi-factor authentication credentials can also be locked to a specific mobile device to guard against an attacker moving the credential to another device and trying to use it to gain access to the enterprise applications. This combination of functionality provides security similar to a hardware token in addition to the cost, usability and maintenance benefits of a software solution.

Figure 2.

CA Advanced Authentication mobile applications



CA Auth ID app CA Mobile OTP app

[1]Ant Allan, research vice president at Gartner. Taken from “Gartner Says 30 Percent of Organizations Will Use Biometric Authentication for Mobile Devices by 2016,” press release, February 4, 2014.

Virtualizing the Desktop—More or Less Secure

Virtualization is not a new phenomenon. The value and benefits have been realized by countless organizations; however more and more companies are exploring virtual desktop infrastructure (VDI) as an alternative to a server-based computing model. VDI hosts the desktop operating system and client applications within a virtual machine running on a backend server and can help organizations save money and increase flexibility. And, although VDI can increase security as confidential data is now stored on the server instead of the user's machine, it also introduces security risk as users could potentially access their applications from anywhere.

VPNs can be used to protect access to these environments and allow users to access them from different locations, and SSO solutions can be used to enable access to every application without having to re-enter passwords. But both of these technologies are still subject to the risks associated with passwords. Incorporating advanced authentication, either directly with the VDI solution or indirectly with the VPN and/or SSO solution, will address this weak link.

CA Advanced Authentication addresses VDI by either integrating with the VPN appliance or directly with the VDI system (e.g., Citrix XenApp). In this case, the process would be nearly identical as for VPN appliances. The VDI system would redirect users to the CA Advanced Authentication login URL, which would authenticate the user and an OTT would be used to validate the authentication.

Section 2:

CA Technologies Multi-Layered Authentication

CA Advanced Authentication provides a layered approach to authentication security. It combines CA Risk Authentication and CA Strong Authentication to improve an organization's ability to authenticate legitimate users and deny access to cybercriminals.

Authentication That Is Convenient, Secure and Cost-effective

In situations where additional authentication security is necessary but an organization is not ready to implement two-factor authentication credentials, risk-based authentication can be a smart, "just-in-time" type of approach. CA Risk Authentication can detect and protect against high-risk access attempts and transactions by analyzing a wide set of factors without requiring any direct input from the end user.

The 2015 Verizon Data Breach Investigations Report found:

- Approximately 37 percent of insider data breach incidents were from end users and only 1.6 percent from system admins.
- In many of the incidents reviewed, the insider abuse was only discovered after the user left the company.

> "Catching insider abuse is not easy. You need to … begin by identifying those core areas and then look for activities to track or places where you need to insert additional auditing and fraud detection capabilities so you can get ahead of the attackers."[1]

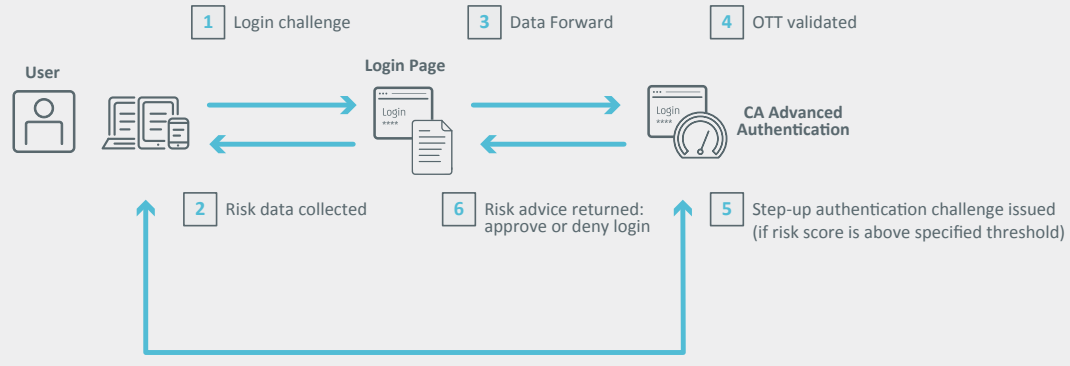
Simply adding a transparent risk-evaluation provides greater assurance that the user is who they claim to be. The risk evaluation produces a risk score that is combined with business policies to determine if any action is required. This allows legitimate users, the majority of the login attempts, to continue uninterrupted because their risk score is low. In the case of an unacceptable risk score where the user's behavior is outside the norm, the user can automatically be required to do step-up authentication to further prove their identity. This could include answering knowledge-based questions or entering an OTP that has been sent (out-of-band via SMS, email or voice) to their mobile phone.

High-risk access attempts can be denied and/or cause an alert that triggers security or service desk intervention if necessary. The organization has the ability to use preset rules and/or add custom rules to control and adjust the risk scoring process to fit their environment.

Figure 3.

Risk analysis can detect and stop inappropriate access on its own to catch fraudulent activity even if credentials have been compromised.

CA Advanced Authentication risk assessment workflow



[1]2015 Data Breach Investigations Report, published by Verizon

Sophistication of fraud continues to increase making it more difficult to distinguish between fraudulent and genuine users. As enterprises expand their applications beyond the perimeter they need more than "black box" risk assessments. The ability to control risk parameters on-the-fly and understand fraudulent and legitimate behavior is essential in any authentication deployment. CA Risk Authentication provides the following:

- **Greater Accuracy:** Using an enterprise-specific model that understands legitimate and fraudulent behavior, we can determine the validity of a user in context of what is normal for that individual. In real-time during authentication, CA Risk Authentication takes a multidimensional view of the login by using elements such as the device characteristics, geolocation, login velocity and historical user behavior.
- **Faster Speed of Change:** Allows enterprises to make changes to rules and business policies on the fly. With access to case information for all logins, an administrator can update authentication policies based on action that triggered step-up authentication or denied login. Policies can be updated or added dynamically as required by the business needs. There is no dependency on the vendor to make changes.
- **Better User Experience:** Can authenticate an employee, partner or contractor without complicated user credentials. Enterprises can use risk-based authentication with simple passwords and only require step up authentication if the login seems risky. This provides a frictionless login experience for most users, improving productivity while reducing the cost of interrupted work time and calls to the help desk.

Versatile Authentication and Multiple Two-Factor Credential Options

CA Strong Authentication provides a broad set of authentication methods that can be applied as appropriate for different applications, user groups and situations, including password, knowledge-based Q&A, out-of-band, out-of-wallet Q&A, OATH-compliant tokens and the unique CA Auth ID and CA Mobile OTP. The CA Auth ID and CA Mobile OTP are secure software credentials that provide two-factor authentication without the cost or inconvenience of hardware. These credentials can be deployed on a computer/tablet or mobile phone providing two-factor authentication, and are protected with a patented key concealment technology called "Cryptographic Camouflage" against brute force and dictionary attacks that attempt to derive the password.

Unbreachable Passwords

The CA Auth ID is a self-contained, PKI-based, two-factor credential that employs a challenge/response mechanism which provides additional protection against password guessing or MITM attacks. This software–based credential is both easy to deploy and simple for users. The one-time enrollment process can be as easy as a few self-service screens or it can be extended to include knowledge-based answers (KBA) or SMS delivery of a one-time code for extra security. After enrollment the user login process is as simple as entering username and password. This password is used to derive the private key is considered to be "unbreachable" because it is not stored on the server or device and is never sent over the wire; it only exists in the user's head.

Authenticate with Mobile Device

The CA Mobile OTP credential is a secure software passcode generator that allows mobile phones, iPads and other PDAs to become a convenient authentication device. If users are familiar with an OTP approach, this is an easy way to upgrade to a software-based solution that is secure, scalable and cost-effective. It supports standards including OATH (HOTP, TOTP) and EMV (CAP/DPA). In situations where an out-of-band authentication method is preferred, CA Advanced Authentication can also send an OTP to the user via SMS/email or voice. This process is a popular way to further verify a user's identity when initially distributing the credential and it can be a good form of step-up authentication as well.

Section 3:

Internal User Enablement with Reduced Risk

Organizations are becoming more global and as a result more internal users are either remote or mobile. Providing an access environment that includes strong authentication is critical to productivity and security. CA Advanced Authentication confirms the identity of employees, contractors and business partners and enables organizations to provide access to applications and sensitive data. CA Strong Authentication provides software and mobile credentials that make it easier to distribute, maintain and scale to a larger user base. The simple enrollment process, familiar login format and self-service features increase adoption and help maintain a high level of user satisfaction. The patented key concealment technology makes it more secure than other software or mobile credentials by reducing the risk of inappropriate access due to a compromised password.

CA Risk Authentication with user behavioral profiling, dynamic rules and immediate access to data provides additional security and even protects the organization if credentials are compromised. This further reduces risk with no impact to the legitimate user because the contextual risk evaluation happens in the background. Together this layered approach can help an organization increase security, meet compliance regulations and reduce administration costs while facilitating the increased productivity that secure remote access enables.

The combination of a strong two-factor credential and background risk evaluation can make it much more difficult for an attacker to gain access to the organization's internal network, corporate applications and confidential data. This is a powerful combination of benefits, any one of which could be used to justify the solution, but together create a compelling business case for any organization. In addition, this type of a secure implementation can also be very helpful for dealing with compliance regulations and auditing requirements.

Section 4:

Next steps

Organizations should take a look at the full spectrum of data and resources that users can access via their applications and develop a risk appropriate authentication strategy. In many situations this will reveal the need for risk-based authentication coupled with strong credentials. The next challenge is to select the best combination of security, cost and user convenience to meet these needs. CA Technologies offers a wide range of strong authentication solutions that provide additional security in a user friendly and cost effective manner.

To learn more about CA Advanced Authentication visit ca.com/us/multifactor-authentication.

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**.

CS200-155581