



Adding Stronger Authentication to CA SiteMinder® Web Access Manager

Solution Guide

May 2009





Adding Stronger Authentication to CA SiteMinder Web Access Manager

Solution Guide

SOLUTION GUIDE

Overview

Enhances CA SiteMinder WAM by adding stronger authentication to user Web access.

Quickly and easily upgrade users to multi-factor authentication without the need to change their familiar username/password sign-on process.

Protects CA SiteMinder WAM-protected consumer and enterprise portals.

Blocks fraud in real time and eliminates the need for expensive hardware tokens or cards.

The CA SiteMinder® Web Access Manager (CA SiteMinder WAM) is a core component of your Web access management strategy. CA SiteMinder WAM provides a centralized security management foundation that enables the secure use of the Web to deliver anytime, anywhere access to applications and data to customers, partners, and employees.

A Weak Link

Username/passwords are the most common way for users to authenticate to Web applications and portals protected by CA SiteMinder WAM. Unfortunately, username/passwords are often a critical weak link in a Web security system. Easily cracked, stolen, or given away, username/passwords used by themselves often lead to identity theft and fraud. Username/passwords also fail to satisfy many industry best practices and regulatory guidelines for protecting user identities and data.

Traditionally, any enterprise wishing to upgrade its CA SiteMinder WAM users to stronger authentication face deploying expensive hardware-based technologies: one-time password (OTP) tokens, smartcards, or USB drives. For enterprises with thousands of users, the cost to deploy hardware-based strong authentication can be prohibitive. Furthermore, these costly technologies also require changes to user behavior which result in significantly higher operational costs because of the increase in the number of calls to the help desk.

Software-Only Multi-Factor Authentication

Arcot WebFort® is a software-only multi-factor authentication solution integrated with CA SiteMinder WAM. WebFort transparently protects and verifies your Web users' identities, without the need for expensive hardware or the need to change your users' familiar username/password-based sign-on process. Its low cost and ease of use enables you to protect all of your customers, partners, and employees from identity theft and fraud with two-factor authentication.

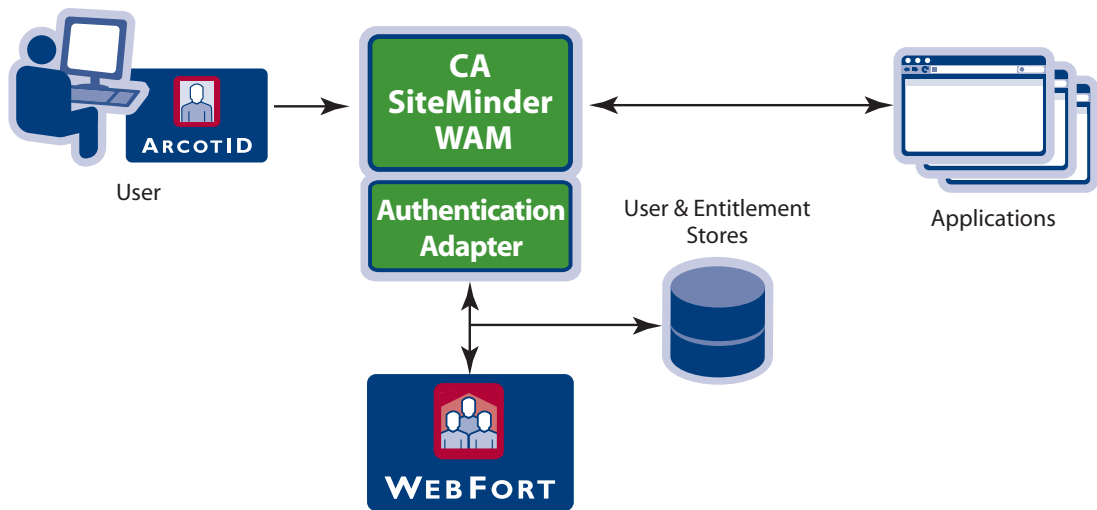
Arcot WebFort delivers multi-factor authentication for CA SiteMinder WAM completely in software. It adds a layer of identity protection and verification to your CA SiteMinder WAM-protected Web applications and portals, without the cost and complexity of OTP tokens or smartcards.

WebFort's software-only form factor also makes it easy to use, deploy, and manage. Adding WebFort to your CA SiteMinder solution does not require changes to your end-user sign-on experience, so there is no need to train your users in new procedures, no end-user involvement in the upgrade process, and no calls to the help desk.

At the heart of the WebFort solution is the ArcotID®, a secure software credential that hides Arcot's sophisticated two-factor authentication technology from your users. It protects the digital identities of your users with proven, patented cryptographic technology. It appears to your users as their same username/password sign-on, but 'behind the scenes' it uses public key infrastructure (PKI)-based challenge/response to verify your users' identity before granting Web access to CA SiteMinder WAM-protected applications and data.

WebFort protects your users from sophisticated Internet threats like Man-in-the-Middle, brute force, phishing, pharming, password cracking, and other attacks. For example, the ArcotID verifies that the user is signing into the domain that issued it before prompting the user for his password, preventing Man-in-the-Middle and other phishing attacks from succeeding. Arcot's patented "Cryptographic Camouflage" protects the user's digital credentials from being compromised by brute force attacks.

FIGURE 1: WEBFORT INTEGRATION ARCHITECTURE



WebFort is also easier and less expensive to deploy to your users, even to consumer users and partners. Its software form-factor gives you complete flexibility for deploying the ArcotID. The most common deployment is in Adobe Flash. Because over 98% of the internet-accessible desktops in the world have Flash installed, there is no software to install on your users' desktops. Other options include "push" deployment as part of a regular software update, user self-service provisioning, or installation on physical media (such as a USB drive).

WebFort's roaming capability ensures that your users maintain their anytime, anywhere access to your CA SiteMinder WAM-protected applications, information, and services. When users are away from the PC they typically use, they can quickly verify their identity through knowledge-based Q&A and gain secure roaming access from any system in the world.

The benefits of adding WebFort to CA SiteMinder WAM include the following:

- *Out-of-the-box integration:* CA SiteMinder WAM's authentication management capabilities make it easy to add Arcot multi-factor authentication to your mix of authentication technologies
- *Improved security:* Protects against new Internet threats like Man-in-the-Middle that defeat One-Time Password (OTP) tokens
- *Reduced risk:* Multi-factor authentication reduces risk of identity theft and online fraud by enabling safe, secure remote access to data and applications from anywhere
- *Improved compliance:* Comply with regulatory policies or industry best practices for two-factor authentication for customers, employees, and partners

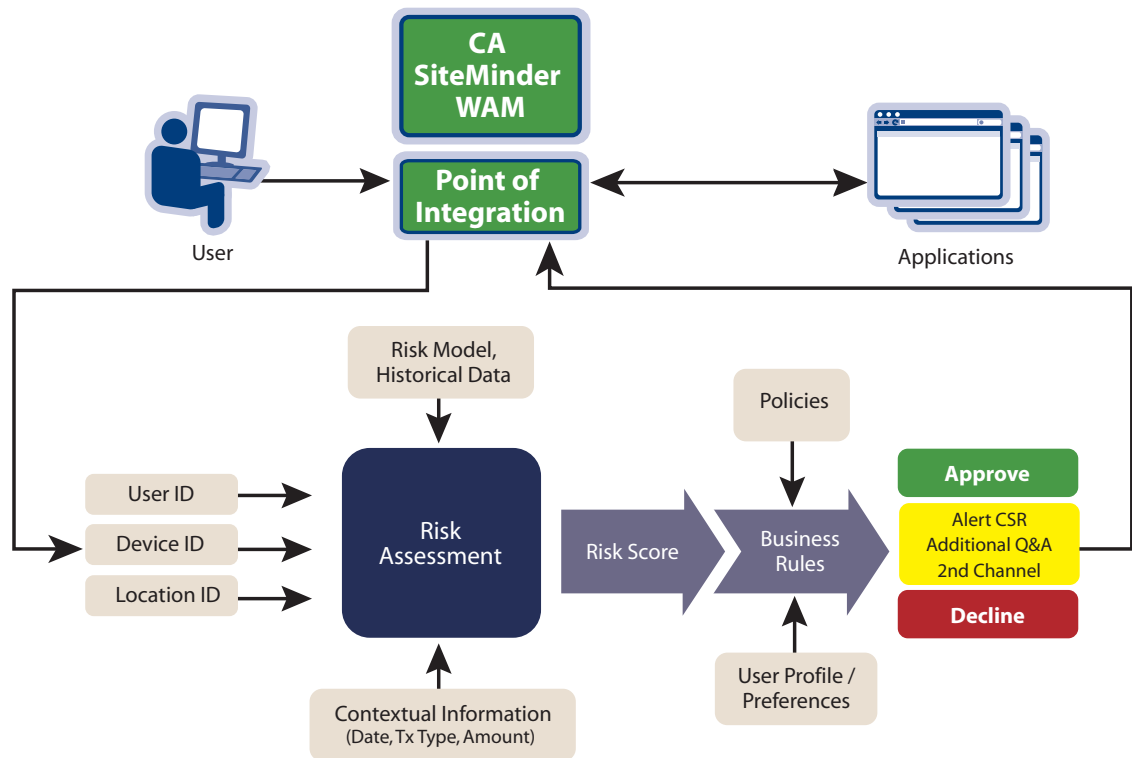
- *Reduced cost:* Arcot WebFort's software-only approach eliminates expensive desktop hardware or tokens. With WebFort, there is no hardware to lose, fail, or break. It provides the lowest cost of ownership of any multi-factor authentication technology on the market today. Software-only and fully self-service provisioning significantly reduces purchase, deployment, and management costs
- *Enhanced user experience:* No change required to familiar user sign-on experience eliminates user confusion and calls to the help desk

WebFort Integration Architecture

When a user requests access to CA SiteMinder WAM-protected application, CA SiteMinder WAM first determines the authentication scheme to use. If the request requires WebFort-based strong authentication, SiteMinder WAM invokes the Arcot authentication scheme. SiteMinder then receives an encrypted challenge from WebFort and issues that challenge to the user's ArcotID. The ArcotID requests the password from user, to sign the encrypted challenge and sends the encrypted signed challenge back to WebFort via the authentication scheme. WebFort authenticates the user, the user receives a CA SiteMinder WAM single sign-on cookie, and gets access to the protected application for which he is authorized.

WebFort never sends the private key or password to the server. It hides all of the sophisticated encryption/decryption processes behind a familiar username/password sign-on page, eliminating calls to the help desk.

FIGURE 2: RISKFORT INTEGRATION ARCHITECTURE



Risk-based or Adaptive Authentication

Arcot also provides RiskFort, a risk-based authentication solution that detects and blocks online fraud in real time. RiskFort works with CA SiteMinder WAM to add an invisible layer of protection against fraud and identity theft. It measures and blocks fraud in real-time, without any interaction with your users.

You can quickly and easily add RiskFort to any consumer- or enterprise-facing portal. It assesses the fraud potential of every online access attempt by examining a range of data collected automatically.

It compares the contextual information with historical data and statistical analysis techniques to identify anomalous activity and calculate a Risk Score. It uses this Risk Score, combined with your unique business policies and each user's profile, to recommend the action to take regarding the sign-on attempt (e.g., approve, decline, require additional authentication, or refer to Customer Service Representative).

RiskFort uses three analytical processes to examine the range of data automatically collected concerning the request:

1. Customizable rules (e.g., device ID, location, IP address range, etc.)
2. Statistical model comparing historical activity profile and fraud data

3. Callouts to other tools, either internal or external (e.g., Fair Isaac's Falcon® fraud manager)

RiskFort also has three features that you can add to complement its core fraud detection capabilities:

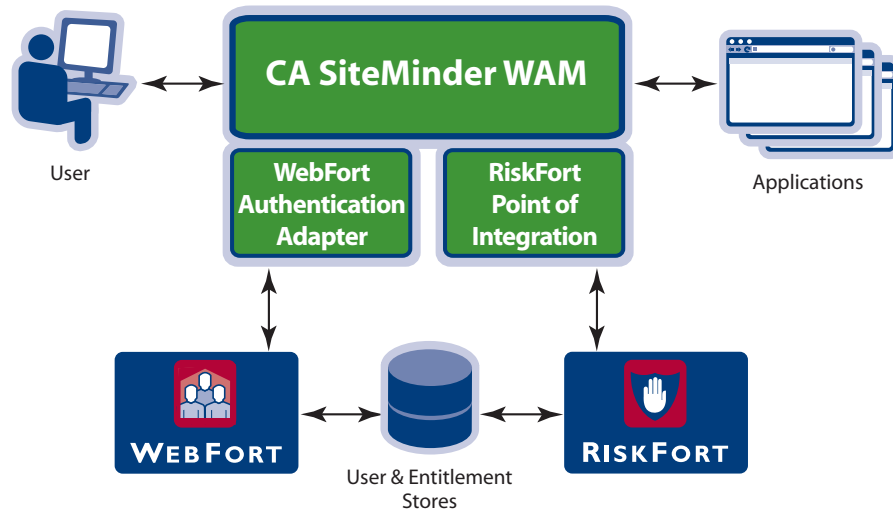
- *A Personal Assurance Message*
Message that provides mutual authentication of the validity of the sign-on site to your user
- *A Scrambled PIN Pad* that prevents malware (such as keystroke or mouseclick loggers) from effectively using a captured PIN, as the order of the keys change with each sign-on attempt
- *Detailed geomapping* of user's location based on IP address

The benefits of adding RiskFort to CA SiteMinder WAM include the following:

- *Ease of installation:* RiskFort installs quickly, without requiring changes to your consumer or enterprise portals
- *Improved security:* Adds an invisible layer of protection to CA SiteMinder WAM-protected data and applications
- *Reduced risk:* Detects and blocks unauthorized users masquerading as legitimate users
- *Improved compliance:* Comply with regulatory policies or industry best practices for stronger authentication than simple username/password

Adding Stronger Authentication to CA SiteMinder WAM

FIGURE 3: WEBFORT AND RISKFORT DEPLOYMENT



- *Reduced cost:* Reduces losses due to fraud and identity theft
- *Enhanced user experience:* Transparent to users, with no change to their familiar sign-on experience

session automatically and transparently, without any involvement with your users. Arcot's software-only approach gives you the right balance of cost, convenience, and strength for enhancing the protection of your Web users.

Benefits of Arcot Solutions

Arcot delivers additional identity protection for your CA SiteMinder WAM-protected Web applications. Whether you want integrated multi-factor authentication, transparent risk-based authentication, or both, Arcot's unmatched authentication expertise adds additional protection to your critical data and applications.

About Arcot Systems

Arcot makes Web transactions safe for millions of users worldwide by verifying and protecting users' identities. Its software-only solutions eliminate the need for expensive hardware or changes to user behavior. Arcot delivers online fraud prevention, strong authentication and e-Document security solutions.

WebFort can quickly and easily add multi-factor authentication to your SiteMinder WAM-protected Web applications and portals, without changing your users' familiar username/password sign-on process. WebFort eliminates the need for expensive tokens or cards, giving you the lowest TCO of any two-factor authentication solution on the market.

About CA

CA (NYSE: CA), one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT. Founded in 1976, CA is headquartered in Islandia, N.Y., and serves customers in more than 140 countries. For more information, please visit <http://ca.com>.

RiskFort can detect, measure, and block online fraud before it can affect your CA SiteMinder WAM-protected applications and data. It collects information on each

About Arcot

Arcot authentication and digital signing solutions make Web transactions and online access safe for millions of consumer, enterprise and e-Commerce users. With Arcot solutions, organizations can transparently deploy stronger authentication without changing user behavior or deploying expensive hardware. Arcot fraud prevention, strong authentication, and e-Document security solutions are delivered on-premise or as SaaS providing the right balance of cost, convenience and strength.

For more information, please visit www.Arcot.com, email sales@arcot.com, or contact your nearest sales office:

Corporate Headquarters, U.S.
Arcot Systems, Inc.
Ph: +1 408 969 6100

United Kingdom
Arcot International
Ph: +44 118 965 7998

Germany
Arcot Deutschland GmbH
Ph: +49 8157 997793

India
Arcot R&D Software Private Ltd
Ph: +91 80 6660 2745



www.arcot.com

Copyright © 2009 Arcot Systems, Inc. All rights reserved. Arcot, Arcot WebFort and ArcotID are registered trademarks of Arcot Systems, Inc. All other trademarks are the property of Arcot Systems, Inc. or their respective owners.