



Versatile Authentication for CA SiteMinder®



Block Identity Fraud in Real-Time
Protect and Verify User Identities

DATA SHEET

Overview

Arcot provides authentication solutions that integrate seamlessly with your CA SiteMinder Web Access Manager. Arcot enhances SiteMinder by adding risk-based authentication and strong authentication to prevent identity theft and fraud.

Arcot allows you to upgrade users quickly and easily to layered authentication, without changing their familiar username/password login process. Arcot's software-only solutions eliminate the need for expensive tokens or cards.

Users keep their familiar login process while Arcot transparently protects and verifies their identity. Arcot offers the right balance of cost, convenience, and strength.

THE CHALLENGE: PROTECTING USER IDENTITIES, SIMPLY AND SECURELY: The most common way for users to authenticate with CA SiteMinder is with username/passwords. Unfortunately, they are also the weak link in any identity management strategy. Easily cracked or stolen, simple usernames and passwords invite identity fraud. Traditionally, any enterprise wishing to upgrade its SiteMinder users to stronger authentication faced deploying expensive hardware-based technologies such as one-time password (OTP) tokens or smart cards.

THE SOLUTION: VERSATILE, SOFTWARE-ONLY AUTHENTICATION FOR SITEMINDER: Arcot RiskFort® and WebFort® are software-only authentication solutions that protect and verify your users' identities. RiskFort detects online fraud automatically, and WebFort prevents identity theft and fraud. Arcot provides hardware-strength protection of your users' identities while keeping the ease of use of a password. Versatile Authentication allows you to apply dynamically the appropriate level of authentication to different groups of users, based on policies, privileges and risk profile.

First Layer: Risk-Based Authentication

RiskFort delivers non-invasive risk-based authentication that detects and blocks identity fraud in real-time, without affecting legitimate users. It measures the fraud potential of every online access attempt to any consumer or enterprise-facing portal or application.

No Change to User Experience

Arcot lets you upgrade from simple username/passwords without changing your users' login experience or your critical business processes. RiskFort analyzes the data it collects without interaction with your users. WebFort hides the sophisticated cryptographic challenge/response from your users, protecting their identity while keeping the simplicity of a password.

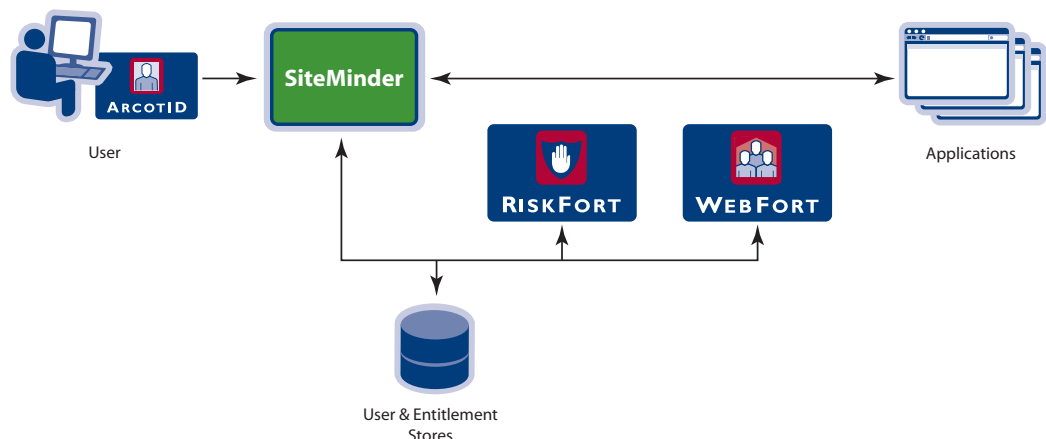
Second Layer: Software-Only Strong Authentication

WebFort provides multi-factor authentication completely in software. It adds hardware-strength identity verification to any username/password login process without the complexity. It enables 'step-up' authentication to ensure that users accessing more sensitive resources use a stronger authentication mechanism.

Lowest Cost of Ownership

Our software-only approach eliminates expensive desktop hardware or tokens. With Arcot, there is no hardware to lose, fail, or break. WebFort provides the lowest cost of ownership of any layered authentication solution on the market today.

SITEMINDER WITH ARCOT VERSATILE AUTHENTICATION



RISKFORT

Server platforms

Operating Systems

- Microsoft Windows Server
- Sun Solaris

Application Server

Interface Support

- JAVA API for J2EE-compliant application servers (e.g., IBM WebSphere, BEA WebLogic, and Apache Tomcat)
- Web Services for Windows .NET platform-enabled and other application servers

User Identification

Data Sources

- LDAP Directories
- SQL Databases

WEBFORT

Desktop Platforms

Browsers

- MS Internet Explorer
- Mozilla Firefox
- Netscape Navigator
- Apple Safari

Operating Systems

- Microsoft Windows
- Mac OS X
- Linux

Server Platforms

Operating Systems

- Microsoft Windows Server
- Sun Solaris

Certificate Authorities

- OpenSSL
- VeriSign OnSite
- MS Certificate Server
- Entrust/PKI
- RSA Keon
- CyberTrust Unicert

Crypto Interfaces

- Microsoft CSP
- PKCS #11

Optional Hardware Security Modules

- nCipher

SITEMINDER WITH ARCOT FEATURES AND BENEFITS

WEBFORT AUTHENTICATION METHOD	BENEFIT
ArcotID	Arcot's patented software credential delivers hardware-strength authentication without changing user behavior or your existing business processes.
PKI Challenge Response	Provides the same strong authentication as a physical smart card or USB security token by holding an X.509 certificate. Integrates with your existing PKI-based applications and infrastructure.
One-Time Password (RADIUS)	Enables you to replace your expensive OTP hardware tokens and replace them with the ArcotID.
Username/Password Against SQL or LDAP Directories	Integrates with your existing user management database/directories, eliminating the need for another database or directory.
Security Assertion Markup Language (SAML)	Enables federated authentication with your existing Identity and Access Management infrastructure.

RiskFort Risk-Based Authentication

Reduce Losses Due to Fraud

RiskFort prevents fraud losses by blocking high-risk transactions before they complete, or requiring additional authentication for unusual transactions.

Match Rules to Your Environment

The customizable rules engine and policy store enables you to configure RiskFort to match your business practices and risk tolerance, rather than forcing you to change your operations to fit your security tool.

Invisible Protection

Your users never have to know that you have RiskFort deployed to prevent fraud. There is no change to their user experience and therefore no calls to the help desk.

Multi-Component Risk Assessment

RiskFort combines three components for unmatched fraud detection capabilities:

- Customizable policy store
- Optional fraud model
- Callouts to other internal or external tools

Fraud Model

Uses statistical techniques, including Bayesian modeling, to compare each transaction against a scoring formula. RiskFort periodically updates the formula based on recent fraud and transaction data.

Callouts

RiskFort can call other internal or external fraud management applications, such as Falcon. You can also aggregate scores from multiple systems to generate one combined score.

WebFort Multi-Factor Authentication

Eliminate Man-in-the-Middle attacks

WebFort prevents Man-in-the-Middle attacks, keeping users safe from Phishers and Pharmers. The ArcotID protects them when One-Time Password tokens and Grid Pads cannot.

Anytime, anywhere access

Your users can download the ArcotID securely while roaming, giving them secure access from anywhere. You can also install the ArcotID on a PC, carry it on a USB drive or smart card, for increased flexibility.

Fully self-contained

There are no additional elements of PKI-based authentication to install or deploy—WebFort contains everything you need. It is a single, integrated solution that eliminates the trauma of past PKI deployments.

Unlimited scalability

WebFort can scale to verify and protect the identity of millions of users.

Future-ready authentication

WebFort provides the foundation for you to upgrade to other valuable business services like secure "push" eStatements, when you are ready.

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



www.arcot.com

Copyright © 2007 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.