



Adding Strong Authentication to IBM Tivoli Access and Identity Management Solution Guide



SOLUTION GUIDE

Overview

Arcot enhances IBM Tivoli Access and Identity Management solutions with strong authentication and simplified user credentialing.

You can transparently upgrade users to strong authentication without changing sign-on behavior.

IBM® Access and Identity Management solutions enable your organization to centralize the management of a wide range of access requirements and policies for your IT infrastructure. You can establish a reliable store of identity information, manage user information and privileges, and enforce access control.

The Weak Link

The most common way for users to authenticate with IBM Access and Identity Management solutions is with simple usernames and passwords.

Unfortunately, simple usernames and passwords are the weak link in any identity management strategy. Easily cracked or stolen, simple usernames and passwords invite identity fraud. Compromised user credentials enable criminals to gain access to your critical network resources by masquerading as legitimate users. Simple usernames and passwords also fail to satisfy many industry best practices and regulatory guidelines for protecting user identities.

Traditionally, any enterprise wishing to upgrade its IBM Access and Identity Management users to stronger authentication faced deploying expensive hardware-based technologies: one-time password (OTP) tokens, smart cards, or USB drives. For enterprises with thousands of users, the cost to deploy hardware-based strong authentication was prohibitive. Furthermore, these costly technologies also required changes to user behavior and business processes. Changes in user behavior create significantly higher operational costs because of the increase in the number of calls to the help desk.

The Solution: Strong Authentication Completely in Software

Arcot WebFort with the ArcotID is a software-only, two-factor, strong authentication solution that protects and verifies your users' identities. The patented ArcotID is a unique software credential that prevents identity theft and fraud. It provides hardware-strength protection of your users' identities while keeping the ease of use of a password.

The ArcotID is the second factor ("something you have") needed for two-factor authentication. You have a range of options for distributing the ArcotID, including a Flash client that installs silently, with no user interaction.

WebFort lets you quickly and easily upgrade your user authentication to strong, two-factor authentication without expensive hardware like OTP tokens. In addition, adding WebFort to your IBM Access and Identity Management environment does not require changes to your end-user sign-on experience or your core business processes. 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. WebFort is easier, faster, and less expensive to deploy than traditional OTP tokens or smart cards.

Arcot Integration with IBM Access and Identity Management

Arcot products integrate with both the Tivoli® Access Manager (TAM) and Tivoli Identity Manager (TIM) to prevent identity theft and fraud, and simplify the administration of your users' digital identities.

Tivoli Access Manager

- *RiskFort* integrates with TAM to block fraudulent access in real-time. It identifies high-risk activity, without any interaction from your users. RiskFort assesses the fraud potential of every authentication attempt and online transaction by examining a range of data collected automatically. It calculates a Risk Score and uses it along with your business rules to approve or decline the transaction, ask for additional authentication, or alert a customer service representative.

RiskFort has three optional features:

- *A Personal Assurance Message*
Message that provides mutual authentication of the validity of the sign-on site to your users.
- *A Scrambled PIN Pad* that prevents malware (such as keystroke or mouseclick loggers) from capturing the PIN, as the order of the keys change with each sign-on attempt.
- *Detailed geomapping* of user's location provided by Quova, an Arcot partner.
- *WebFort* integrates with TAM to protect and verify your users' identities by adding strong, two-factor authentication to the sign-on process. It enables 'step-up authentication' for TAM to ensure that users accessing more sensitive resources use a stronger authentication mechanism. Your users' sign-on process is the same username and password they use today. WebFort adds hardware-strength authentication to TAM via the ArcotID, a unique patented software-only credential that protects users identities from brute-force attacks and Man-in-the-Middle phishing threats.

Tivoli Identity Manager

- *WebFort* integrates with TIM to simplify the identity provisioning process by enabling the issuance, revocation, and management of software-only ArcotIDs to your users through one interface.

Benefits of Adding Arcot Solutions to IBM Access and Identity Management

RiskFort

- Measure risk of each authentication attempt and transaction automatically
- Invisible to legitimate users
- Blocks fraud in real-time before identity fraud can occur

WebFort

- Software-only is significantly less expensive to deploy and manage
- Upgrades users to strong authentication without changing sign-on experience
- Integrates with any application to preserve existing business practices
- Single, customizable solution for management of digital IDs
- Easy to provision digital IDs to employees, partners, and customers
- Enable transition to strong authentication, digital signing, and encryption

Integration Architecture

RiskFort: Block Identity Fraud for TAM

When a TAM user attempts to sign on, TAM redirects the request to the RiskFort server. RiskFort analyzes a range of data collected with no user interaction, such as:

- Customizable rules (e.g., device ID, location, IP address range, etc.),
 - Statistical model comparing historical activity profile and fraud data
 - Callouts to other tools, either internal or external (e.g., Falcon)
- RiskFort uses this data to create a Risk Score, and recommends action on the sign-on attempt, based on the score (e.g., approve, decline, require additional authentication, or refer to Customer Service Representative).

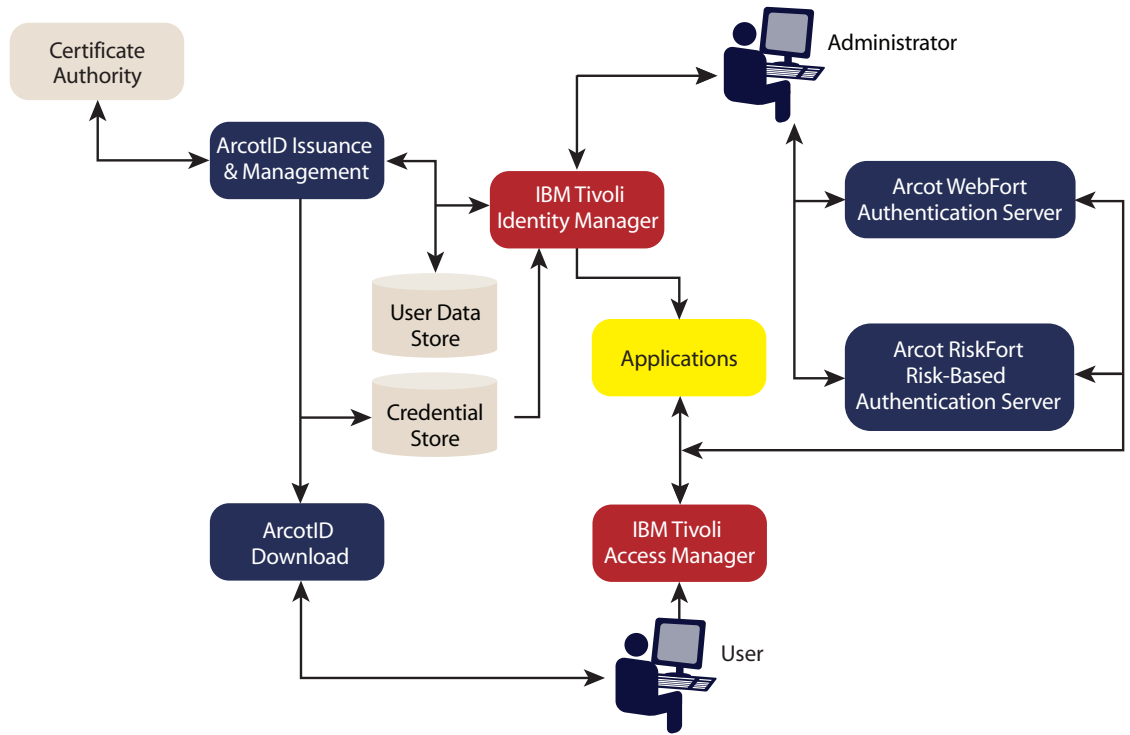
WebFort: Strong Authentication for TAM

When a TAM user attempts to access a protected web application or file, WebSEAL redirects your user to a sign-on page. This sign-on page contains a hidden "challenge" to which only the ArcotID can respond correctly. Your user enters his password to unlock the ArcotID, which then provides a "signed challenge" to the sign-on page. WebFort validates the "signed challenge" from the ArcotID, passes the user's credential to the WebSEAL server. Your TAM policy server examines the user's privileges and allows TAM WebSEAL to grant him access if appropriate.

WebFort: Simplified Identity Provisioning for TIM

When the TIM server receives a request for creating an ArcotID for a user (e.g., an administrator makes the request through the TIM administrative GUI), the Tivoli Directory Integrator (TDI) receives the request and the assembly line needed to generate the Arcot ID. A step in the assembly line uses the custom Arcot connector that makes a request to the WebFort server using Web Services. The TDI returns the result of the operation to TIM and TIM returns the operation result to the caller. The user then receives an email with a one-time activation code and a link to pick up his new ArcotID.

FIGURE 1: INTEGRATION ARCHITECTURE



About Arcot Systems

Arcot Systems is a leading provider of risk-based authentication, strong authentication, digital signing, and cardholder authentication solutions. The company makes online transactions safe for millions of customers by blocking fraud and protecting access. Arcot technology defends against Internet threats including phishing, man-in-the-middle, and spyware. Its 100% software authentication solutions eliminate the need for hardware tokens and complex sign-on processes providing customers with strong, PKI-based authentication with the simplicity of a username/password interface. For more information about Arcot, visit www.arcot.com.

About IBM

IBM is the world's largest information technology company, with 80 years of leadership in helping businesses innovate. Drawing on resources from across IBM and key IBM Business Partners, IBM offers a wide range of services, solutions, and technologies that enable customers, large and small, to take full advantage of the new era of on demand business. For more information about IBM, visit www.ibm.com.

About Arcot

Arcot is the cloud authentication leader. Our fraud prevention, strong authentication, and e-Document security solutions make Web transactions and online access safe for millions of consumer, enterprise, and e-Commerce users.

Organizations can transparently deploy stronger authentication and allow users to conveniently authenticate from any computer or mobile device. Arcot solutions deliver 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.