



# WebFort Performance Brief

## Performance and Scalability for Millions of End-Users

### PERFORMANCE BRIEF

#### Overview

Arcot WebFort is a 100% software, two-factor, strong authentication solution. WebFort lets you upgrade from simple username/passwords without changing your users' login experience or your critical business processes.

WebFort is a high performance authentication server that supports both password and strong two-factor authentication. The patented ArcotID "Software Smart Card" authenticates with WebFort to deliver PKI-strength two-factor authentication, completely in software.

WebFort integrates with your existing IAM, SSO or VPN applications quickly and easily. It enables you to meet regulatory or policy requirements for strong authentication while maintaining the low cost of software.

**INTRODUCTION** Strong authentication solutions are rapidly becoming a necessity for Internet-facing applications. However, wide-scale authentication deployments must do more than provide security; they must be able to scale with the global organizations that deploy them. Arcot WebFort meets the three critical requirements of a strong authentication solution: Robust security, Ease-of-use and Performance. Arcot WebFort provides strong, two-factor authentication while maintaining the familiar username/password interface that users see every day. At the same time, WebFort delivers performance unmatched by other strong authentication solutions and proven scalability to millions of users.

#### The Authentication and Authorization Process

Any remote authentication solution must go through three steps to allow access to a resource: Secure the communications channel, identify and authenticate the user, and authorize the transaction.

##### 1) Secure the communications channel

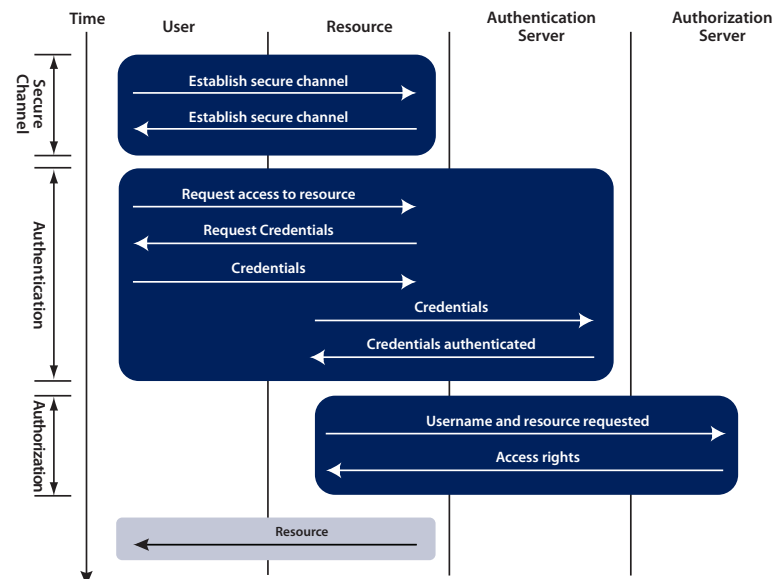
Organizations must protect authentication data from potential eavesdropping, phishing or "Man-in-the-Middle" attacks. If an attacker intercepts data in transit, he can steal the credentials and reuse them at his convenience. Most organizations secure the communications channel using

the popular SSL protocol, the basis for secure web communications. SSL encrypts data in transit and can also provide server authentication.

##### 2) Identify and authenticate the user

Users authenticate with solutions ranging from simple usernames and passwords to biometric data or public-key infrastructure (PKI) technology. Regardless of the technology, the authentication solution must identify and authenticate the user. In general, strong authentication solutions require two of three possible factors:

**FIGURE 1: REMOTE AUTHENTICATION PROCESS**



- Something you know, such as a password or PIN
- Something you have, such as a token, smartcard or mobile phone
- Something you are, such as a fingerprint, voiceprint, face or retinal scan

### 3) Authorize the transaction

Once the solution identifies and authenticates the user, the final step is to authorize the action itself. The authorization process is outside the scope of this paper focusing on Arcot WebFort performance. Nonetheless, it contributes to the overall latency of the authentication process and is part of any real-world deployment.

Each of these steps contributes to the overall performance of the authentication solution. Figure 1 shows the timeline for a typical deployment with the three steps of the authentication and authorization process and the essential components of the solution. The following sections will focus on the identification and authentication phase.

### Performance Factors in Authentication

The two most important performance factors in an authentication solution are scalability and latency. Scalability describes how well the solution provides services to thousands or millions of users and performs hundreds or thousands of authentication transactions a minute. Latency describes the delays introduced in the system by the different components that make up the authentication service.

#### Scalability

Most authentication solutions are “vertically scalable” or scalable within a single machine. Adding memory, processors, and disk space are examples of vertical scaling to increase performance or capacity. Scaling vertically by adding memory and disk is the simplest, as it does not require any special capabilities on part of the software designers. Scaling vertically by adding CPUs requires more sophisticated software development expertise. For this reason, many older applications, or applications developed by less-skilled developers will experience difficulties when run on a multi-CPU machine.

A “horizontally scalable” application virtualizes the application across multiple machines by using load balancers and/or custom programming. Horizontal scalability is more

sophisticated than vertical scalability and if done correctly, can provide virtually unlimited scalability.

#### Latency

Latency or lag is a key factor in determining the usability of a solution to the end-user. Users are very sensitive to the amount of time they need to wait between actions. Without feedback on the wait time, a user may perform unnecessary actions (such as re-submitting credentials) that can interfere with the authentication process. If the lag is long enough, users may end up calling a support line or even abandoning the online session completely. Both of these actions result in increased costs to the organization. To manage costs and ensure a superior user interface, a well-designed authentication solution must provide low latency.

### High-Performance Authentication with Arcot WebFort

WebFort is the core of Arcot’s authentication architecture. To meet the rigorous security, availability, and data integrity demands of the financial services industry, Arcot designed WebFort from the start to provide the strongest security and performance possible. To provide authentication services to millions of users, Arcot designed WebFort with virtually unlimited horizontal scalability, unparalleled ease-of-use and extremely low latency.

#### Virtually Unlimited Scalability

Arcot WebFort provides excellent vertical scalability through increasing memory, disk and processors. It achieves full-featured horizontal scalability with additional local or remote servers. Horizontal scalability provides performance gains as well as high-availability features for critical deployments. A host of advanced features provides these capabilities:

##### *Stateless Servers*

WebFort eliminates the need to store server state information, allowing deployments behind load balancers. This provides two benefits:

- 1) Increased capacity and the ability to deploy WebFort in high-availability (HA) configurations
- 2) Deployment of WebFort in multiple geographic locations to avoid the latency of long-haul links to a central data center

### *Connection Pooling*

All Arcot products use proprietary connection pooling technology to avoid expensive connects and reconnects to database servers, crypto devices, remote servers and other servers and devices.

### *False Contention Avoidance*

Large Symmetric Multiprocessing Systems (SMPs) often suffer from false contention. Using proprietary techniques, Arcot designed the WebFort data structures to eliminate this problem on multi-CPU SMP systems.

### *Built-in Failover Technology*

The ability to quickly and transparently fail over to back-up servers is critical in any high-availability scenario. WebFort automatically fails over to a backup system in the event of the failure of any component of the service such as the database, crypto module or certificate authority. Database failover is especially critical and WebFort minimizes transaction failure even during the failover. Organizations can also configure WebFort to fail-back to the primary database upon its restoration.

## **Low-Latency Authentication**

The key measure of performance from a user perspective is latency. Using proprietary techniques, Arcot provides latency comparable to that of a username/password system with the security of two-factor authentication.

Transmission delays and the time required to process the request on the server are the largest components of latency. Some transmission delays are unavoidable because of the inherent latency in Internet routing, but efficient algorithms can reduce the time required to process requests on the server. Arcot's experienced development team has developed extremely efficient services using a number of sophisticated techniques:

### *Cutting-edge parallel programming techniques*

WebFort features fully multi-threaded servers, advanced thread/data synchronization and advanced communication techniques. WebFort also has a patented search index that allows the authentication server to maintain very fast transaction speeds. These features enable WebFort to maintain its transaction speeds even when scaled across multiple CPUs and multiple servers. These transaction speeds are critical in maintaining low latency during peak periods of activity.

### *Efficient client access interface and protocols*

Proprietary binary protocols and highly efficient parsers optimize the communications between the ArcotID Software Smart Card and the WebFort Authentication Server. These factors reduce the time required to decode and encode messages sent between components.

### *Optimized database interface*

Inefficient database interaction can slow even the fastest software to a crawl. Arcot's database programming expertise enables the creation of highly optimized database schemas and SQL statements that allow exceptionally efficient database interactions.

### *Data cache*

Accessing the database is much slower than accessing local memory. The WebFort server caches often-used data to minimize database interactions.

### *Multi-CPU-aware memory managers*

Most large SMP systems come with memory managers that quickly become the bottleneck due to lock contention. Arcot has an extensive understanding of this issue and employs custom multi-CPU memory managers to avoid this problem.

## **Performance Case Study**

A large US bank with several million online users recently chose Arcot WebFort after substantial and thorough performance testing. Arcot had already demonstrated the ability to scale to millions of users with other customer installations. However, the bank wanted to calculate metrics such as the number of login transactions per second and the latency introduced by the Arcot solution. To do so, it needed to test WebFort in its environment.

The bank already had a standard secure channel, a login mechanism and an authorization service for their consumer banking clients. However, to ensure that the system would meet its performance requirements, the bank needed to run performance tests. It required measurement of both the baseline performance of the existing authentication solution, as well as the performance of the solution after incorporating WebFort.

### Test Architecture

The test architecture consisted of Sun V280 (2 CPU) and V440 (4 CPU) systems. Mercury LoadRunner generated the session load, which ranged from 600 to 1200 simultaneous authentication sessions.

The joint Arcot/Bank testing team conducted the performance tests in three stages:

- 1) Establish a baseline to measure the performance of the system prior to using WebFort.
- 2) Test the change in performance after introducing WebFort authentication into the system.
- 3) Obtain real-life performance statistics on an optimized, production-quality, multi-node system with a simulated load of up to 1200 authentication transactions per second.

For the Stage 1 test, Netegrity SiteMinder provided both authentication and authorization services. For the Stage 2 test, Netegrity continued to provide authorization services but WebFort provided strong authentication.

During the Stage 2 test, WebFort and Netegrity SiteMinder ran on the same Sun V440 system. The impact of this was

minimal however — although the tests simulated 600 simultaneous users, CPU load averages for all systems had very little change (see Figure 3). The change was less than the margin of error of the baseline measurements when compared with baseline measurements taken without WebFort.

For the Stage 3 test, the team used the deployment shown in Figure 2. Once again, Mercury LoadRunner generated the user load, this time with 1200 simultaneous authentication sessions. Stage 3 was representative of a real-world deployment with multiple servers hosting the authorization service, the database and the WebFort service.

### Test Results

WebFort made a very strong showing in the tests, and introduced a very small latency of between 145 and 165 milliseconds. This translated to an overall overhead of only 5%, well within the requirements set by the bank. The lack of difference between the second and third tests shows that there was very little overhead introduced by scaling WebFort horizontally. This proves that WebFort can continue to scale to deployments of very large size without degrading performance. These results illustrate how WebFort's design allows superior scalability without introducing any substantial latency.

**FIGURE 2: PERFORMANCE TESTING CONFIGURATION**

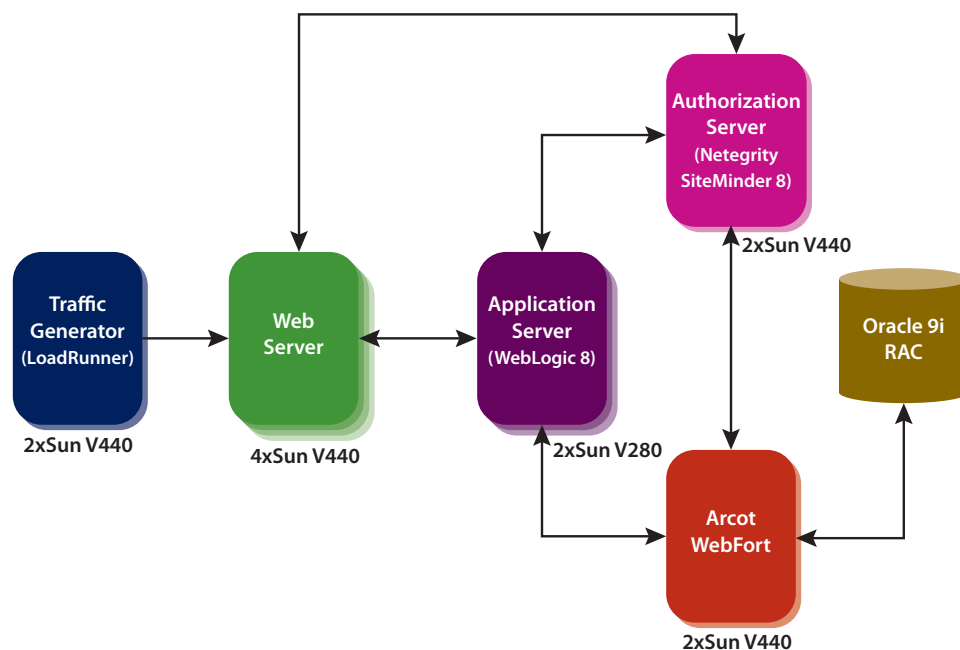
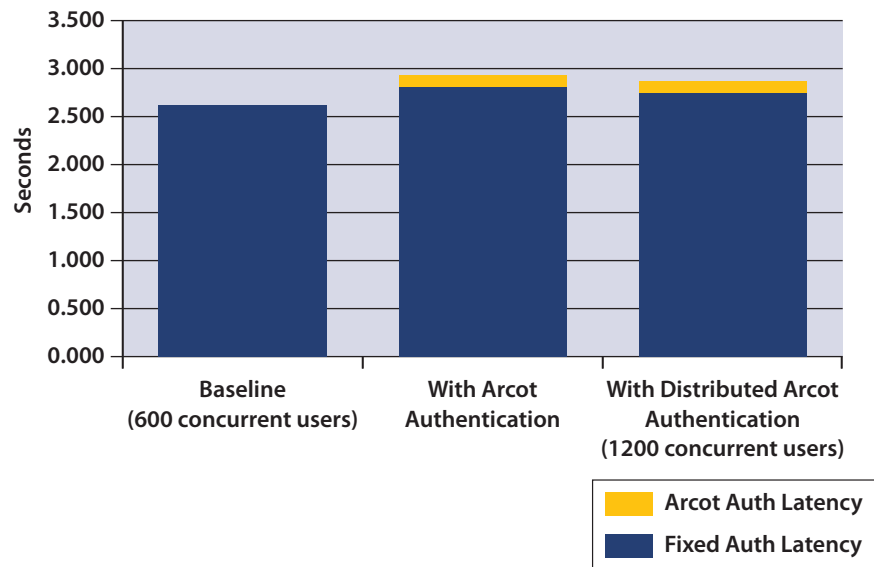


Figure 3 shows the latency of the base system both before and after integrating WebFort strong authentication. The test data originates from the Stage 1, Stage 2 and Stage 3 deployment scenarios respectively. In Stage 2, the same server co-located all authentication and authorization services.

**Conclusion**

Arcot WebFort provides organizations with the strong authentication they want with the scalability and low-latency they need. Arcot's development team has created a sophisticated high-availability solution that scales to current deployments in excess of 15 million users, while meeting the low-latency requirements demanded by the users of today's authentication infrastructures.

**FIGURE 3: LATENCY OF ARCOT WEBFORT AUTHENTICATION SOLUTION**



**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](http://www.Arcot.com), email [sales@arcot.com](mailto: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](http://www.arcot.com)

Copyright © 2010 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.