QUEST SOFTWARE®
*Smart Systems Management*

**DATASHEET**

# Quest® Authentication Services *for Siebel*

## Efficiency, Security, and Compliance for Siebel from Active Directory

Organizations that rely on enterprise applications such as Siebel often need to maintain multiple user identities and authentication methods across a range of critical resources. Users typically have an Active Directory account and Windows logon for access to the Windows-based applications required for day-to-day work. However, when a critical application must run on a non-Windows server and it isn't natively equipped to authenticate against Windows standards, users require additional logins. Consequently, IT must create, maintain, and audit an entirely separate set of identities, which leads to inefficiency, security issues, and compliance concerns.

Quest Authentication Services provides the solution to these challenges. In addition to its core capability of integrating Unix, Linux, and Mac systems with Microsoft Active Directory for centralized authentication, Authentication Services also provides integration for key applications. Through a built-in security adapter for Siebel, Siebel installations running on Unix and Linux can authenticate with the same Active Directory login using the same security rules and standards that are already in effect for the Windows login.

Authentication Services is the first and only solution specifically designed to leverage the generic Siebel Security Adapter Interface 3.00 API to integrate Siebel with Active Directory. Without Authentication Services, organizations running Siebel will integrate with Active Directory ineffectively through a generic LDAP security adapter or through their own "custom" security adapter.

## Benefits

- Authenticate to Siebel applications running on Unix from Active Directory in a simple, efficient, and secure manner
- Achieve optimal integration through a Siebel Active Directory security adapter on Unix and an Apache module for single sign-on
- Enforce Active Directory password and access control policies to Siebel applications running on Unix or Linux
- Use Active Directory group memberships for Siebel roles

## Active Directory Authentication

Authentication Services extends the same integrated Windows authentication (IWA) provided for Siebel running on Windows to Siebel running on Unix and Linux. Because Unix and Linux systems are actually "joined" to the Active Directory domain, Authentication Services for Siebel can provide IWA to Siebel running on Unix and Linux.

### CORE DIFFERENTIATOR

- Active Directory authentication for Siebel running on Unix and Linux
- Siebel access control based on Active Directory rules and groups
- Single sign-on

## Advanced Password Security

Typical LDAP-bind password validation practices require additional security measures (such as the implementation of TLS/SSL and certificate infrastructures) to properly support password change. Authentication Services, with its Kerberos integration, overcomes these shortcomings by seamlessly supporting Siebel password change, password policy enforcement, and password expiration notification well beyond the limitations of the LDAP-only approach.

## Siebel Role Management

Authentication Services for Siebel also enables you to manage Siebel roles using Active Directory groups. This approach greatly simplifies management by eliminating the need to separately manage and maintain Active Directory groups and Siebel roles for the same set of users.

## Siebel Account Management

Authentication Services makes managing Siebel user accounts more efficient, more secure, and more compliant. Siebel roles can be managed through the Active Directory Users and Computers MMC interface; Active Directory account creation and administrative passwords sets can be administered from the Siebel management interface.

## Ability to Leverage Active Directory beyond Windows

Authentication Services for Siebel fully leverages the site topology of Active Directory to distribute load and provide redundancy for Siebel authentication operations. It includes a disconnected mode for use when an Active Directory domain controller may become unavailable and supports the full range of Active Directory capabilities, including support for multiple forests and domains, Windows 2000 and 2003 at any Forest functional level, and even two-way, one-way, and no-way trusts. In addition, Authentication Services provides the flexibility to offer benefit-laden deployment in both schema-based and schema-less options.

## Single Sign-on

For environments where Siebel is running on an Apache web server, Authentication Services for Siebel integrates with the Siebel Web Server Extension for single sign-on to Siebel from Active Directory.

## About Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit **www.quest.com** for more information.

## SUPPORTED ENVIRONMENTS

### Siebel running on:

- HP-UX
- IBM AIX
- Sun Solaris
- Linux

### Support for Siebel Versions

- 7.5
- 7.7
- 7.8
- 8.0+

QUEST SOFTWARE®
*Smart Systems Management*

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.