QUEST SOFTWARE®

DATASHEET

Quest® Authentication Services Single Sign-on for SAP: Increase the Security, Privacy and Compliance of Your SAP Data

Quest Authentication Services (formerly Vintela Authentication Services) SAP BC-SNC Certified Single Sign-on for SAP Solution Enables Unique Security Capabilities for SAPgui Applications on the Windows Desktop

Mission-critical Data Demands Mission-critical Security

For many organizations, SAP applications and services are mission-critical. Compliance, security and economics demand control over user access, authentication to resources and the protection of data as it moves across the network.

Some of the biggest challenges facing organizations that rely on SAP, include:

- Ensuring that only the right people have access to data
- Guaranteeing that those people can access SAP when they need to
- Ensuring that mission critical information is secure as it moves across the network

SAP applications often must meet the strict standards demanded by regulatory compliance, internal controls defined by governance policies and corporate best practices. But how can an organization make that happen in today's increasingly complex multi-platform environment? Achieving unified authentication, data protection and single sign-on for SAP has been complex and difficult to implement—until now.

The Single Sign-on for SAP solution from Quest Software leverages the secure, compliant and scalable infrastructure offered by Microsoft's Active Directory (AD) Using the security and identity infrastructure already in place for your Windows environment, Authentication Services Single Sign-on for SAP allows users to transparently authenticate their SAP gui applications with the credentials acquired at network logon

Single Sign-on for SAP

AD provides a true single sign-on environment for Windows resources. Through its use of the industry standards Kerberos and LDAP, AD provides a compliant, secure and scalable infrastructure for authentication, authorization and access. For users of SAP on Unix systems, Authentication Services from Quest Software provides the same capability. It allows Unix and Linux systems to "join" the AD domain, which extends the compliant and secure AD-based authentication, for SAP to SAP on Unix servers.

Consequently, the workload required of the SAP administration team can be dramatically reduced, as they no longer need to be distracted by password management issues. At the same time, this integration also results in a superior user experience and can increase the security by protecting SAP data in transit between the client and the server using advanced encryption technologies.

KEY BENEFITS

Single Sign-on for SAP through Quest Authentication Services:

- Provides true AD-based single sign-on for SAP running on Unix or Linux
- Eliminates the transmission of users' passwords over the network
- Securely encrypts SAP data, while it is transported over the network
- Simplifies deployment without the need for PKI or certificate infrastructure
- Provides an audit trail for SAP authentication activities with AD

SAP® Certified
Integration with SAP NetWeaver®

SAP® Certified
Integration with SAP NetWeaver®

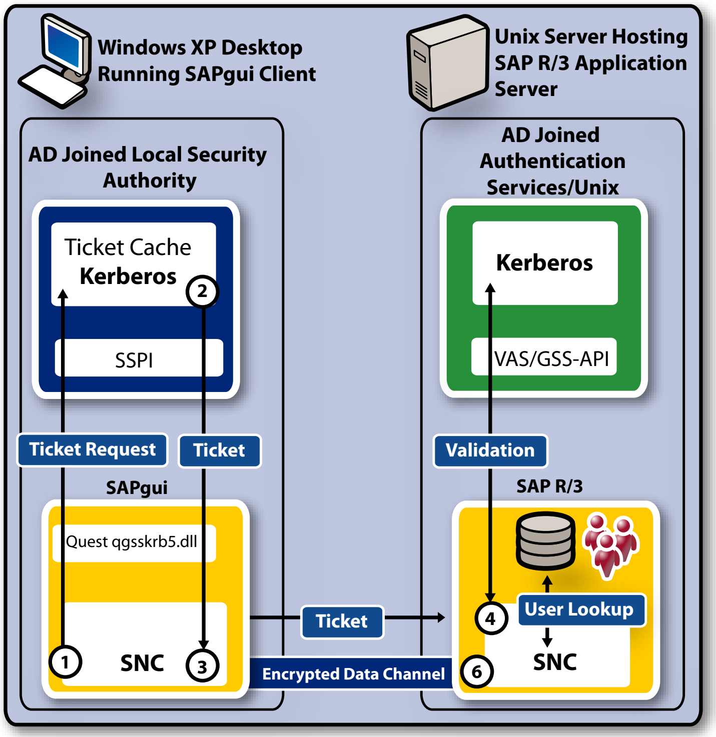
The efficiency, end user satisfaction and control provided by single sign-on for SAP through Active Directory and Authentication Services, yields significant ROI. This solution helps to reduce the help desk burden caused by multiple identities and multiple logins, as it reduces the total cost-of-ownership and leverages the existing investment in AD and SAP for maximum benefits.

Implementing Authentication Services Single Sign-on for SAP:

- Provides true AD-based single sign-on for SAP running on Unix or Linux
- Eliminates the transmission of users' passwords over the network
- Can be configured to perform data integrity checks on session data
- Optionally encrypts SAP data, while it is transported over the network
- Simplifies deployment without the need for PKI or certificate infrastructure
- Provides an audit trail for SAP authentication activities with AD

Authentication Services integrates Unix and Linux hosts, running SAP with Windows-based clients through robust, standards-based security. The SAP SNC interface provides SAP clients and servers a platform-independent security and authentication infrastructure, which fully leverages native Windows and Unix security mechanisms. Windows-based SAP clients can exchange secure authentication tokens, using Kerberos tickets with Unix-hosted SAP R/3 servers.

The Single Sign-on for SAP solution is comprised of both an Authentication Services-configured Unix server which hosts the SAP R/3 application, and a desktop component which provides GSS-API services to the desktop SAPgui client. Together with Active Directory, this solution is certified by SAP for the BC-SNC 4.0 interface. It is the only certified SAP solution that also provides complete integration of Unix identities with Active Directory, providing the additional benefit of allowing the Unix and SAP administrators who must log on to the R/3 server to also use their Active Directory username and password credentials—or transparently authenticate with a single sign-on-enabled terminal client on a Windows desktop.


Windows XP Desktop Running SAPgui Client
Unix Server Hosting SAP R/3 Application Server
AD Joined Local Security Authority
Ticket Cache
Kerberos
SSPI
AD Joined Authentication Services/Unix
Kerberos
VAS/GSS-API
Ticket Request
Ticket
Validation
SAPgui
Quest qgsskrb5.dll
SNC
SAP R/3
User Lookup
SNC
Ticket
Encrypted Data Channel
1
2
3
4
6

1. SAPGUI requests a Kerberos Service Ticket via Quest's qgsskrb5.dll which translates GSS API requests to SSPI
2. A Windows KDC generated ticket is returned
3. SAPGUI client connects to the SAP R/3 Application Server passing the returned ticket
4. SAP R/3 Application Server validates the ticket via the Authentication Services Unix GSS API libraries
5. The Kerberos tickets UPN is mapped to SAP R/3 account
6. An (optionally) encrypted data channel is established using information provided in the Kerberos ticket

True Single Sign-on for SAP

Authentication Services natively implements Kerberos and LDAP on Unix and Linux systems in the same way those standards are used in Windows. It enables a single "trusted realm" that includes Unix, as well as Windows, allowing them to use the same Kerberos tickets used for Windows authentication. This creates true single sign-on between Windows desktops and Unix systems. Authentication Services also enables single sign-on for GSS-API aware applications, such as SAP, DB2, Apache and ssh.

Quest's Resource Central Web site provides customized implementations of tools, such as openssh, PuTTY and Apache. These solutions are configured to provide single sign-on and to allow users to leverage this security and single sign-on infrastructure at a more integrated level than they could with a certificate/PKI-based product. The site also includes guidance documents describing other application integration procedures.

More about Quest Authentication Services

Authentication Services provides a cost-effective, enterprise-proven and standards-based alternative to cumbersome and complex synchronization or meta-directory solutions. With Authentication Services, the same infrastructure, processes and personnel that are already in place to manage Windows resources can now be extended to support and manage a full range of Unix and Linux systems, as well as a growing number of applications including SAP. The result is enhanced security and a clear path to enterprise-wide regulatory compliance.

Benefits of this cross-platform integration of non-Windows platforms and applications with AD include:

Single Sign-on for Heterogeneous Systems: Authentication Services natively implements Kerberos and LDAP on Unix and Linux systems in the same way those standards are used in Windows. It allows AD to create a single, "trusted realm" that includes Unix, Linux and Windows. This creates true single sign-on between Windows desktops and Unix/Linux systems, and for GSS-API aware applications, such as SAP, Apache and ssh.

Enterprise-wide Identity Management Based on an Existing Infrastructure: Authentication Services provides the seamless capability to extend the already deployed and highly robust AD infrastructure to the rest of the enterprise. Rather than purchasing, deploying and supporting an additional infrastructure, tools and technologies for non-Windows systems, this product allows organizations to consolidate all identity and authentication management in AD—the preferred platform that's already in place.

Simplified Identity Management: By integrating Unix and Windows accounts into a single identity store (namely AD), Identity Management complexity is greatly reduced. Provisioning and de-provisioning of Unix accounts can be performed with the same tools and at the same time as Windows. Additionally, other advanced identity administration capabilities, such as password management, audit and role management, can be centralized on an AD-based infrastructure.

Advanced Data Protection: Authentication Services supports both DES and RC4 encryption. This provides the users of Authentication Services with the choice of cryptographic algorithms to protect the privacy of data while it is "in flight".

About Quest Software, Inc.

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest solutions for application management, database management, Windows management, virtualization management, and IT management, go to **www.quest.com**.

SAP® Certified
Integration with SAP NetWeaver®

QUEST SOFTWARE®

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.

© 2011 Quest Software, Inc.
ALL RIGHTS RESERVED.

Quest, Quest Software, the Quest Software logo are registered trademarks of Quest Software, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. DSW-SSO-4SAP-US-KS