QUEST SOFTWARE®
Smart Systems Management

Quest®
Authentication Services

Compliance | Single Sign-on | Simplifying Identity Management

Quest Authentication Services provides enterprise-wide access, authentication and authorization for Unix, Linux, and Mac systems by using Active Directory (AD), the existing identity management infrastructure for Windows resources. Authentication Services' patented technology allows non-Windows resources to become part of the AD trusted realm, and extends AD's security, compliance and authentication capabilities to Unix, Linux, and Mac.

Authentication Services is the undisputed leader in the Active Directory bridge market with nearly 1,000 customers and more than 5 million deployed licenses. Only Authentication Services provides the functionality, flexibility, and scope of integration to meet the needs of the most complex and demanding heterogeneous global organizations.

Administration, Configuration, and Management

Authentication Services has robust and flexible Unix utilities, as well as flexible deployment options. It contains a powerful set of tools for creating and managing your AD bridge, including:

- Product configuration and licensing
- Guidance to help with initial set up and integrating systems with AD
- A broad range of migration and deployment options
- Pre-migration assessment and preparation
- NIS migration tools
- Group Policy and local Unix users and groups management tools
- Simplified and compliant auditing and reporting
- Strong authentication for non-Windows systems

BENEFITS

- Eliminates complexity by allowing Unix, Linux, and Mac systems to participate as "full citizens" in Active Directory
- Consolidates the administration of AD-enabled systems and AD bridge functionality around a single, powerful console
- Delivers strong authentication as part of the AD bridge solution
- Expands auditing, alerting, and change tracking to AD-enabled Unix, Linux, and Mac systems
- Provides centralized authentication and single sign-on
- Facilitates the migration of all systems and users to a single Active Directory-based infrastructure
- Simplifies security and compliance
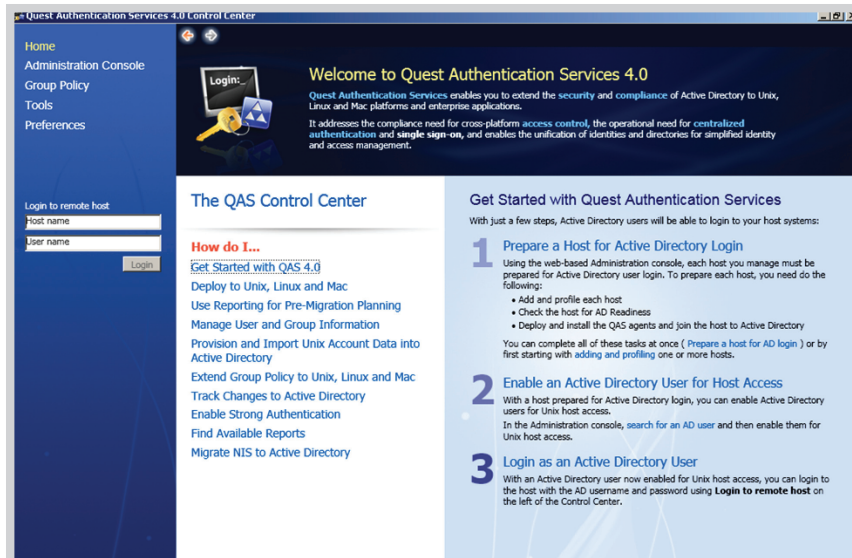- Extends Group Policy to Unix, Linux, and Mac OS X systems

Figure 1 *The Quest Authentication Services Control Center*

Strong Authentication

Authentication Services includes licenses for powerful AD-based, one-time password (OTP) strong authentication across all supported Unix, Linux, and Mac platforms. In addition, Authentication Services extends Windows-based smart cards to Unix and Linux and supports third-party OTP solutions.

Audit, Alerting, and Change Tracking

Only Authentication Services gathers the vital data demanded by auditors. Authentication Services enables you to audit, alert, and provide a detailed change history of Unix-centric information managed by Active Directory.

Compliance

Authentication Services uses the same industry standards as AD to provide a compliant alternative to multiple identity stores and points of authentication, as well as non-compliant directories, such as NIS. It also quickly and easily gathers the critical information demanded by auditors, and seamlessly facilitates strong authentication for non-Windows systems.

Migration

Ideally, most heterogeneous organizations want to consolidate into one secure and robust directory for all of their systems. Authentication Services can help you quickly achieve that goal by streamlining the process of integrating Unix, Linux, and Mac systems and users to the AD domain. It also facilitates a fast and accurate migration from multiple authentication mechanisms, identities and directories into a single AD-based infrastructure. Capabilities include:

- Mapped User Mode provides an elegant alternative to a full migration. It allows the migration to proceed at its own pace while quickly resolving the most pressing compliance requirements. Mapped User Mode enables organizations to achieve immediate compliance with no impact on the Active Directory schema.

- Unix Personality Management creates alternate Unix "personalities" to define profiles in AD for different systems, using standard schema attributes based on the default AD schema definition.

- Ownership Alignment Tool simplifies the time-consuming final step of resolving user-ID conflicts at the end of a migration. It provides a flexible tool set for aligning the ownership of conflicting files; this allows you to quickly re-align user namespace conflicts before, during or after your primary migration to AD.

- Full RFC 2307 NIS Map Support provides full support for users migrating their NIS infrastructure into Active Directory's RFC 2307 NIS maps, enabling them to completely retire their existing NIS infrastructure. RFC 2307 is supported with advanced NIS map import wizards, NIS map editors for Windows, and full RFC 2307 support in the Authentication Services NIS proxy.

- Unix Account Import Wizard imports users and groups to personalities from sources such as NIS, local files, or remote shells. It also enables you to choose sophisticated matching criteria (for linking to account principal) from pop-ups. This greatly simplifies the tedious work of migrating users into AD.

Enterprise Group Policy

Authentication Services provides an easily implemented, infinitely scalable, and natively integrated extension of the Windows Rights Management Service Group Policy to Unix, Linux, and Mac systems. Through this framework, you can leverage the existing Group Policy extensions built into the product, or develop your own based on the simple ADM template methodology, or the more capable client-side extensions. Authentication Services includes generic scripting, file copying and customization, as well as a collection of powerful pre-packaged Group Policies and flexible policy management. In addition, the product leverages existing Windows security policies, making AD entirely authoritative for Unix, Linux, and Mac access control. Authentication Services includes a powerful Group Policy interface for Mac OS X systems that provides control over the entire range of Mac policy and preferences, including support for third-party applications through Preference Manifest integration. Authentication Services also audits and tracks changes to Group Policy Objects.

Active Directory for Unix, Linux, and Mac

Authentication Services seamlessly extends an existing AD infrastructure to the rest of the enterprise. Authentication Services natively integrates Unix, Linux, and Mac systems to allow them to act as full citizens within AD and benefit from AD's security and compliance advantages. Key capabilities include:

- Extends AD password policy to Unix, Linux, and Mac

- Supports the most complex AD environments including multiple domains, cross-forest trusts, and nested groups

- Leverages AD's ARC4 strong encryption (128-bit keys) for Unix, Linux, and Mac to enhanced security

- Synchronizes Unix system clocks with AD

- Supports the RFC 2307 schema definition as implemented in Windows Server 2003 (R2)

- Supports custom schema configuration as well as implementation options for pre- R2 schemas without extension.

Centralized Authentication and Single Sign-On

Authentication Services natively implements Kerberos and LDAP on Unix, Linux, and Mac systems in the same way they are implemented in Windows. In addition, it provides single sign-on for many applications (including SAP and Siebel), a powerful application programming interface (API)that allows you to add single sign-on to internally-developed applications and guidance for creating single sign-on to a number of popular applications (such as DB2, PuTTY, Samba, and Apache).

Centralized Access Control

Authentication Services enables you to configure access rules using several options:

- Local, file-based access lists that determine what users can access on the Unix and Linux machines (down to the level of the individual services). These can then be centrally managed through Group Policy.

- Unix Personality Management helps control access by defining the user namespace for a given set of computer hosts

- Windows security policies and the User Workstation features can provide granular, per-user access control to Unix computer objects in AD.

Simplified Identity Management

Authentication Services enables you to simplify identity management based on your existing AD investment. Using Authentication Services, AD-based identity management solutions— including those for provisioning, password management, strong authentication, privileged account management, and auditing and reporting— from Quest and other vendors can be naturally extended to non-Windows systems. Authentication Services can also work with an existing IAM framework to reduce the number of systems that require custom integration and individually managed connectors.

Extensive Cross-Platform Support

Authentication Services provides centralized authentication support for the widest range of Unix, Linux, and Mac platforms including Solaris, IBM AIX, HP-UX, SuSE, RedHat, Fedora, VMware, Mac OS X, and others. For a complete list of supported platforms refer to http://www.quest. com/authentication-services/supported-platforms.aspx
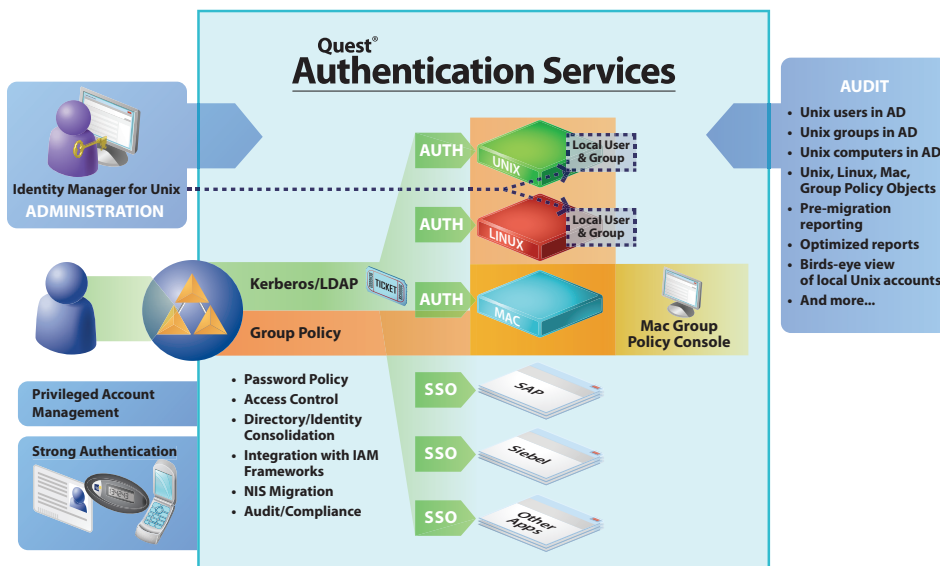
About Quest Software, Inc.

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.