IDENTITY MANAGEMENT

Simplifying Identity Management

QUEST SOFTWARE®

Identity Management

What Does Identity Management Mean to You?

Every organization faces the challenge of maintaining control over systems and applications while ensuring appropriate user permissions are in place. This is the very core of identity management and a major factor in compliance initiatives.

In many organizations, identity management requires authentication and authorization capabilities for a large mix of computing environments, and comprehensive administrative capabilities such as provisioning, password management, and auditing. Managing and updating user access privileges can be complicated, as users may require access to varied and incompatible systems and applications—each with its own authentication mechanisms and identity stores. In addition, best security practices, as well as local and national legislation, often require that corporations carefully track and review user access and administrator actions for auditing purposes.

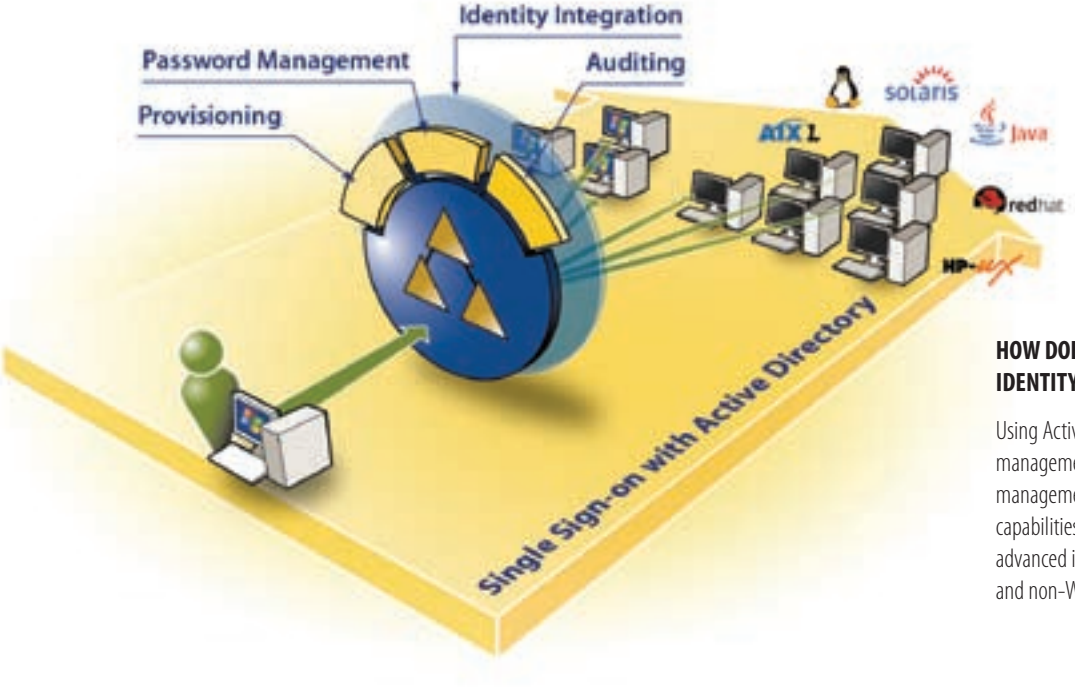
Given these complex and challenging requirements, compliance through identity management demands a large portion of IT's focus and budget.

THE COMPLEXITY OF IDENTITY MANAGEMENT

As companies introduce new technology, or as employees join, leave or move within an organization, the complexity of user identity management grows. Something as simple as assigning access privileges to a single user for Windows resources—a task that is virtually painless thanks to Microsoft Active Directory—can quickly become costly and error-prone when it must be performed for thousands, or tens-of-thousands of users. When the same users require authentication and access to other platforms, such as Unix, Linux and Java, the complexity of identity management grows exponentially and the potential for compliance violations and security degradation increases as well.

Solutions that address identity management may be a mix of native tools from Microsoft and other platform vendors, point solutions that address specific tasks (such as audit or password management on specific platforms) or large framework solutions that address the entire range of identity management concerns. No matter what solution a company uses, organizations can benefit from an integrated, systematic approach to simplifying identity management and supporting compliance.

Quest offers powerful tools that extend Active Directory to non-Windows systems, simplifies Active Directory management and allows Active Directory to be the foundation for identity management initiatives across platform barriers. Quest's identity management offerings help simplify identity management, regardless of the type of implementation involved.



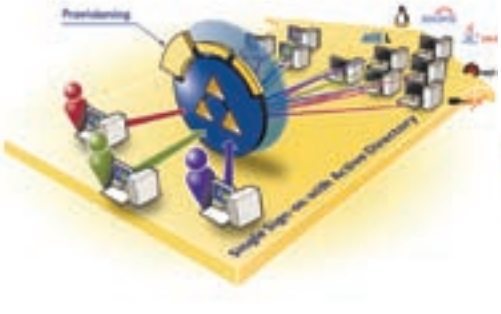
HOW DOES QUEST SOFTWARE SIMPLIFY IDENTITY MANAGEMENT?

Using Active Directory as a foundation of identity management, Quest Software simplifies identity management by extending native Active Directory capabilities to non-Windows platforms, and adding advanced identity administration capabilities for Windows and non-Windows systems alike.

Active Directory as a Foundation of Identity Management

With the growth of Windows as the core platform for business computing, Active Directory has quickly become the dominant access and authentication solution for 80 percent (and growing) of organizations[1]. Active Directory provides one of the most secure, scalable and compliant infrastructures for authentication available today. It provides a true single sign-on environment for Windows resources, as well as a foundation for advanced access capabilities such as federation.

Now, advanced identity administration capabilities such as provisioning, password management, and auditing for compliance can dramatically increase the value of Active Directory as a foundation for comprehensive identity management. Imagine the value of powerful, automated provisioning and role management in Active Directory, integrated with data generated by an organization's HR system. Or, the increased efficiency of the help desk now that they can provide users with self-serve password reset capabilities. Complete the advanced identity administration picture by adding powerful auditing and compliance capabilities that provide a dynamic view of activities in Active Directory, user rights and Active Directory status.



USER PROVISIONING—automates the management of the identity lifecycle through Active Directory-based tools that improve the provisioning, de-provisioning and re-provisioning of users in Active Directory - including Unix, Linux and Java users

PASSWORD MANAGEMENT—streamlines password management through Active Directory-based self-serve capabilities, which can also be extended to Unix, Linux and Java systems

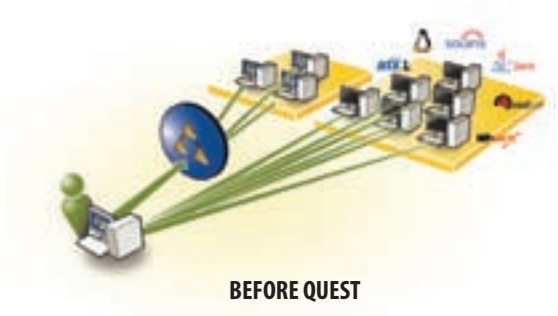
AUDIT AND COMPLIANCE REPORTING—tracks and reports on access, authentication and authorization for Active Directory including non-Windows systems

Extending Native Active Directory Capabilities to non-Windows Platforms

Much of the complexity and inefficiency of identity management, as well as compliance initiatives, is based on the fact that although Windows systems and users may all be members of a single, powerful infrastructure (Active Directory), nothing similar exists for Unix, Linux or Java systems. The end result is multiple (dozens, hundreds or even thousands of) identity stores that require management. Authentication in the non-Windows world enjoys neither the security and compliance nor the scalability and efficiency of Active Directory.

1 From Gartner, Inc., "Ten Recommendations for Microsoft's Active Directory in 2006," John Enck, December 2005.

Imagine the potential cost-savings, security gains and compliance benefits that could be achieved if Unix, Linux and Java authentication could be performed from the same secure infrastructure, using the same user identities and credentials used for Windows systems. Suddenly, one of the most complex and costly aspects of identity management becomes one of the simplest, most secure and compliant.



BEFORE QUEST

AFTER QUEST

REDUCED SIGN-ON—allows Unix, Linux and Java systems to participate in the same "trusted realm" as Windows users and computers.

Extending Advanced Identity Administration Capabilities to non-Windows Platforms

Naturally, the benefits of advanced identity administration capabilities—provisioning, password management and auditing—can be extended to non-Windows systems that have joined the Active Directory domain. Once again, very complex and costly processes such as platform-specific password management or directory auditing can be consolidated into a powerful, scalable infrastructure that is already in place. Now, when a new user joins the organization, an initial entry in the HR system can automatically generate (provision) the correct entries in Active Directory and grant appropriate access to all Unix, Linux and Java resources simultaneously.

QUEST IDENTITY MANAGEMENT

"Vintela Authentication Services meets the mixed-environment challenge for a few users or hundreds-of-thousands of users. It lets Linux and Unix (i.e., IBM's AIX, HP-UX and Sun Microsystems' Solaris) clients authenticate against a Windows Active Directory server while providing single sign-on (SSO) functionality. Any tool that can reduce the management complexity of mixed environments is worth careful consideration. If you need to integrate Linux and Unix with Active Directory, Vintela Authentication Services is a good choice."

—David Chernicoff,
Windows IT Pro,
September 2004

"Because ActiveRoles Server enables us to grant granular rights, we can more comfortably delegate certain functions and only grant rights according to specific job functions."

—Jeff Duldulao
Supervisor, Network Security
Independence Community Bank of New York (ICBNY)

"Vintela Authentication Services increased security. We have fewer accounts to manage and now we can leverage our already secured AD infrastructure. It also reduced our help desk calls and improved staffing. . . Thanks to this product, I can tap into the relatively abundant pool of Windows administrators to manage the entire enterprise. Now my Unix money goes toward important Unix administrative tasks, not password management."

—Kirk Patten,
IT Director,
RotaDyne, Inc.

CAPABILITIES	QUEST PRODUCTS
Identity Integration	**Vintela® Authentication Services** allows you to manage Unix and Linux accounts with Microsoft's directory service — Active Directory. **Vintela® Single Sign-on for Java** allows you to manage Java application accounts with Active Directory.
Reduced Sign-on	**Vintela Authentication Services** and **Vintela Single Sign-on for Java** allow you to create a single sign-on (or reduced sign-on) "trusted realm" where Unix, Linux, and Java systems participate in the same authentication mechanism as Windows users and systems.
Provisioning	**ActiveRoles™** automates and improves the provisioning, re-provisioning, and de-provisioning of users in Active Directory. **Vintela Authentication Services** and **Vintela Single Sign-on for Java** allow you to extend these provisioning capabilities to Unix, Linux and Java application users. **Group Policy Manager** allows you to test, compare, update and rollback Group Policy Objects (GPOs) for better security and control of your IT infrastructure. **Group Policy Extensions for Desktops** allows desktop administrators to remotely manage Outlook and user profiles, security group membership, configuration settings, network connections and scheduled tasks. **Vintela Authentication Services** extends Group Policy to Unix and Linux configuration files.
Role Management	**ActiveRoles** supports role-based delegation of Active Directory administrator privileges. **Vintela Authentication Services** and **Vintela Single Sign-on for Java** allow you to extend this role-based administration capability to the management of Unix, Linux and Java application users.
Password Management	**Password Reset Manager** reduces help desk costs by enabling your users to reset their own passwords. **Vintela Authentication Services** and **Vintela Single Sign-on for Java** allow you to extend this self-service password reset capability to Unix, Linux and Java application users.
Auditing	**Reporter** automates the collection and reporting of the data required for configuration change audits and security assessments of Windows and Active Directory infrastructure. **InTrust® for Active Directory** provides comprehensive, detailed, real-time auditing of all changes to Active Directory and Group Policy Objects (GPOs) including changes to Active Directory configuration and GPO settings. **Vintela Authentication Services** and **Vintela Single Sign-on for Java** allow you extend Active Directory audit capabilities to Unix and Linux systems and Java applications. **InTrust** helps you collect, analyze, report, and generate real-time alerts for all relevant access-related events across heterogeneous systems.

Simplify Identity Management

Regardless of the methods an organization may already be using—native Active Directory, task or platform-specific tools, or comprehensive frameworks—Quest Software can simplify the way organizations approach identity management. Quest can extend the power and compliance of Active Directory — and leverage the identity management capabilities within Active Directory — by integrating it with non-Windows systems. Quest enables organizations to automate provisioning, password management and auditing across platforms.

By working with Quest, organizations can use their existing technologies and current skills to address the challenges of identity management. The end result is greater operational efficiency, increased security and a path to compliance all based on core infrastructure they already own.

For more information on how Quest Software can help organizations like yours simplify identity management, visit www.quest.com/identitymanagement.

APPLICATION MANAGEMENT | DATABASE MANAGEMENT | WINDOWS MANAGEMENT

About Quest

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at **www.quest.com**.

QUEST SOFTWARE®

Please refer to our Web site for regional and international office information.

Corporate headquarters: 5 Polaris Way • Aliso Viejo, California 92656, U.S.A. • U.S. and Canada: +1.949.754.8000
www.quest.com