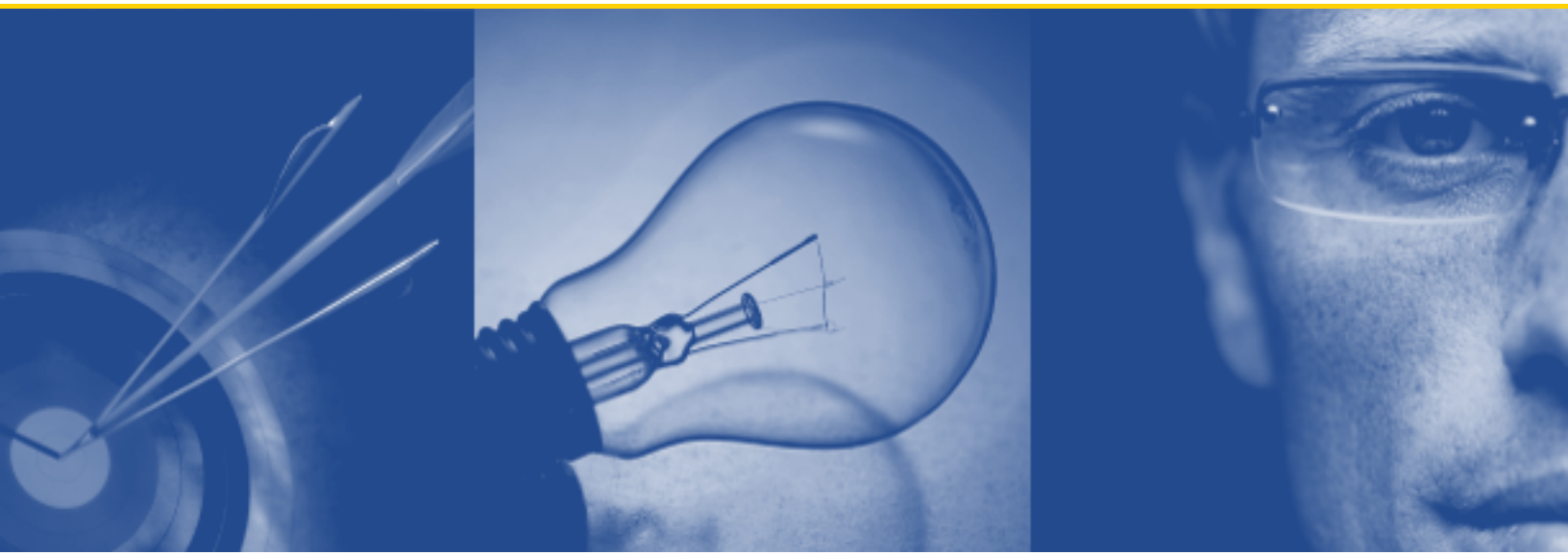
QUEST SOFTWARE®

The Power of One

A Simplified Approach to Identity and Access Management

Written by
Quest Software, Inc.



WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

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

Updated—August 18, 2008

CONTENTS

INTRODUCTION

Today's enterprise faces complex and diverse information systems. Gone are the days of a single, ultra-secure system that were accessed by a select few employees.

With the proliferation of the personal computer, and the networking of those computers, the number and types of systems that are accessed—as well as the number of employees who must be granted access—have grown exponentially.

This paper explains the access and identity challenges that arise in modern heterogeneous environments, and how the Quest One Identity Solution addresses these challenges.

THE COMPLEXITY OF MODERN INFORMATION SYSTEMS

Let's begin by examining the shape of a modern IT environment.

Systems

Today's enterprise can include any of the following systems, each with its own purpose and access requirements:

- **Windows systems** – Microsoft's server operating system, Windows Server, and its key authentication mechanism, Active Directory (AD), house a high percentage of the user identities at the vast majority of enterprise organizations.
- **Unix and Linux** – Most organizations also run Unix or Linux systems. Typically, these systems run enterprise applications and databases that either pre-date the dominance of Windows, or have been deemed to run better on the Unix or Linux platform.
- **Macintosh** – Many organizations also run Macintosh as the desktop choice for a portion of their user base. These users may be isolated from the dominant AD identity infrastructure.
- **Legacy systems** – While growth has slowed, the importance and proliferation of mainframe and mid-range systems are still significant. Typically, these systems are vital to successful operations—due to the critical nature of the data and processes they house and replacing them with Windows or Unix-based systems is out of the question.

Applications

The above platforms run many different applications, including:

- **Enterprise applications**. Heading the list of mission-critical applications are those that we will call “enterprise applications.” Examples of enterprise applications are ERP systems such as SAP, Siebel, and others; financial applications; and Human Resources applications such as PeopleSoft. Often, either by necessity or choice, these applications run on Linux or Unix while the main desktop computing platform is Windows. Access to these applications must be highly controlled yet extremely flexible.
- **Databases**. The backbone of all these platforms and applications is the data. Oracle, DB2, SQL, Sybase, and other databases that may support any of the applications listed above.
- **Other applications**. Beyond enterprise applications, an organization may have any number of additional critical applications to address its unique needs. Whether these applications are industry-specific, home-grown, or custom-built, they often include built-in access control options that may not integrate with the mechanisms of the underlying operating systems and other applications. Access to these applications may be hard-wired or web-based, and it may be restricted to specific employees, open to all employees, available to partners, or even include customer-facing components.

Many enterprises have grown organically—adding platforms and applications when needed—without consideration to the additions’ long-term impact on the other systems. Each system functions as an island unto itself without integration or interoperability with the rest of the enterprise. This is especially true when it comes to user identity and access.

THE PRINCIPLES OF IDENTITY AND ACCESS MANAGEMENT

IT systems and applications exist in order to help organizations avoid risk or make money. The need to achieve those goals is firmly rooted in the principles of identity and access management. These principles are:

- **Authentication** – In order to access any system or application, users must be identified by proving to the system that they are who they say they are. Usually this is accomplished by combining a unique identifier (typically a username) with something only the users should know (typically a password). Many organizations choose to augment this type of authentication with a second factor: something the users have (such as a smart card or a one-time password token). In cases where extreme security is required, organizations can add a third factor: something the users are (such as a fingerprint, retinal scan, or face or voice recognition).
- **Authorization** – Once the system accepts the user login, the users and admins should be granted appropriate access only to the systems, applications, and data required to do their jobs—no more, no less. Authorization becomes particularly challenging, and more important, when access stretches beyond the traditional bounds of the physical network. Providing appropriate access for remote workers coming in via the Internet, and for partners or others that are not under the control of the organization's IT department, is critical.
- **Administration** – In order to facilitate authentication and authorization, the following steps for identity administration must be followed:

    - **Provisioning** – The identity must be set up with all the appropriate rights, group memberships, and attributes required to authenticate and authorize. In a diverse environment, the provisioning process typically must be performed separately on each system and application where the user needs access.
    - **De-provisioning** – Even more critical than initial provisioning is the de-provisioning process. When a user leaves an organization, security and compliance demand that access be terminated as quickly as possible. If the user has access to many systems, de-provisioning can be a tedious and error-prone process.
    - **Password management** – This includes the processes and policies surrounding resetting passwords and the complexity and longevity of those passwords.
    - **Role management** – This includes the processes and policies associated with executing authorization.
    - **Auditing** – Organizations need to track and report on identity attributes and the status and history of authentication, authorization, and access.

THE CHALLENGE OF MULTIPLE IDENTITIES

The mere fact that authentication, authorization, and administration must be controlled for every identity for every user in the enterprise creates the majority of identity and access management challenges.

> *According to Aberdeen Group:*
>
> *"The current research indicates that about nine out of 10 (88%) enterprise users have multiple work-related passwords."*[1]

When each system or platform in an organization functions autonomously with separate authentication, authorization, and administration policies, each user of the systems may need to have dozens of identities.

As an example, an organization with ten separate systems, each with its own directory (and its own processes, policies, and rules) could have:

- 10 passwords per user that must be individually managed and reset
- 10 places to provision and de-provision a user
- 10 separate directories
- 10 sets of policies
- 10 places to audit for access control

THE NEED FOR COMPLIANCE

In recent years, a number of government regulations (such as Sarbanes-Oxley), industry initiatives (such as PCI), and best-practices frameworks (such as ITIL) have established formal requirements for maintaining information security. These requirements also include standardized penalties for failure to comply. In the identity and access management arena, compliance is defined by three common themes:

- **Auditing** – Often the biggest compliance burden is "proving" compliance and discovering areas of deficiency. The more complex and diverse an enterprise is, the more difficult it is to audit the identity environment by documenting all aspects of identity (authentication, authorization, and administration).
- **Access control** – Every regulation demands accountability for access. Organizations must prove that the entitlements that users possess are appropriate, controlled, and based on secure authentication and authorization practices. Access control must be enforced and audited for local users as well as those coming in over the Internet.
- **Segregation of duties (SOD)** – SOD requires, among other things, that an individual whose role includes unlimited access to a key data source or system cannot be responsible for auditing that system.

Causes of Compliance Deficiencies

Some of the most common compliance deficiencies are caused by the inconsistency and lack of interoperability associated with disparate systems and applications. The following deficiencies are the most common:

- **Password policy** – Compliance requirements generally demand the most secure and consistent password policy possible. But in a heterogeneous environment, without very careful planning, password policies may become inconsistent and difficult to manage; each system or application may have its own password complexity, expiration, and longevity rules. For example, legacy systems may have a limit on password length, while some applications may provide the power to enforce granular complexity and length rules.

  Having different password policies on different systems and applications leads to security issues. It's not uncommon for a user in a large organization to be required to change a password weekly or monthly. If the password requirements on each system or application are different, users end up having multiple passwords that are difficult to remember, so they write down their passwords on a sticky note stuck to their monitor, or, worse still, opt for the easiest possible password to remember (and thus the easiest to crack).

- **Non-secure authentication practices** – Many regulations demand user authentication that is more secure than traditional password-based logins. Unfortunately, the same factors that make it difficult to enforce consistent password policy across a diverse environment also make it very difficult to implement strong authentication for all systems and applications that require it. Instead, organizations often have a mix of authentication practices—some strong, some not. As a result, users often find themselves saddled with a variety of smart cards, tokens, or other strong authentication tools. Worse still, some systems fail to require strong authentication when it is demanded or recommended by regulations.

  Aberdeen Group reports:

  "Strategies which are based on establishing and enforcing consistent policies for user authentication correlate most highly (64% of Best-in-Class organizations) with current investments in strong user authentication."[2]

- **Delays in user de-provisioning** – Slow user account deactivation may be the most common compliance deficiency. Aberdeen's recent benchmarking study revealed:

  "100% of best-in-class companies de-provisioned employees within four hours, while 58% of industry average companies took over twenty-four (24) hours."[3]

  If you run only Windows, de-provisioning a user is as simple as deactivating a single account in Active Directory. But if users have access to multiple platforms and applications, each with its own identity repository and user accounts, de-provisioning means deactivating many accounts, often manually, on a box-by-box or directory-by-directory basis. The situation is further complicated if different IT teams must be involved. On some systems (for example, mainframes and Unix), the only administrators with sufficient rights to deactivate an account are the highly compensated (and very busy) senior administrators. Therefore, user accounts remain active long after an employee has left the company, a risky compliance and security practice.

The bottom line is, in today's IT environment, compliance—and the penalties associated with non-compliance—is often the driver that motivates organizations to finally take the steps to control their identity and access management systems, processes, and policies. Strategies and technologies that may have previously been difficult to justify in the budget are now supported by highly motivated management with "compliance" money to spend.

APPROACHES TO IDENTITY IN THE HETEROGENEOUS ENTERPRISE

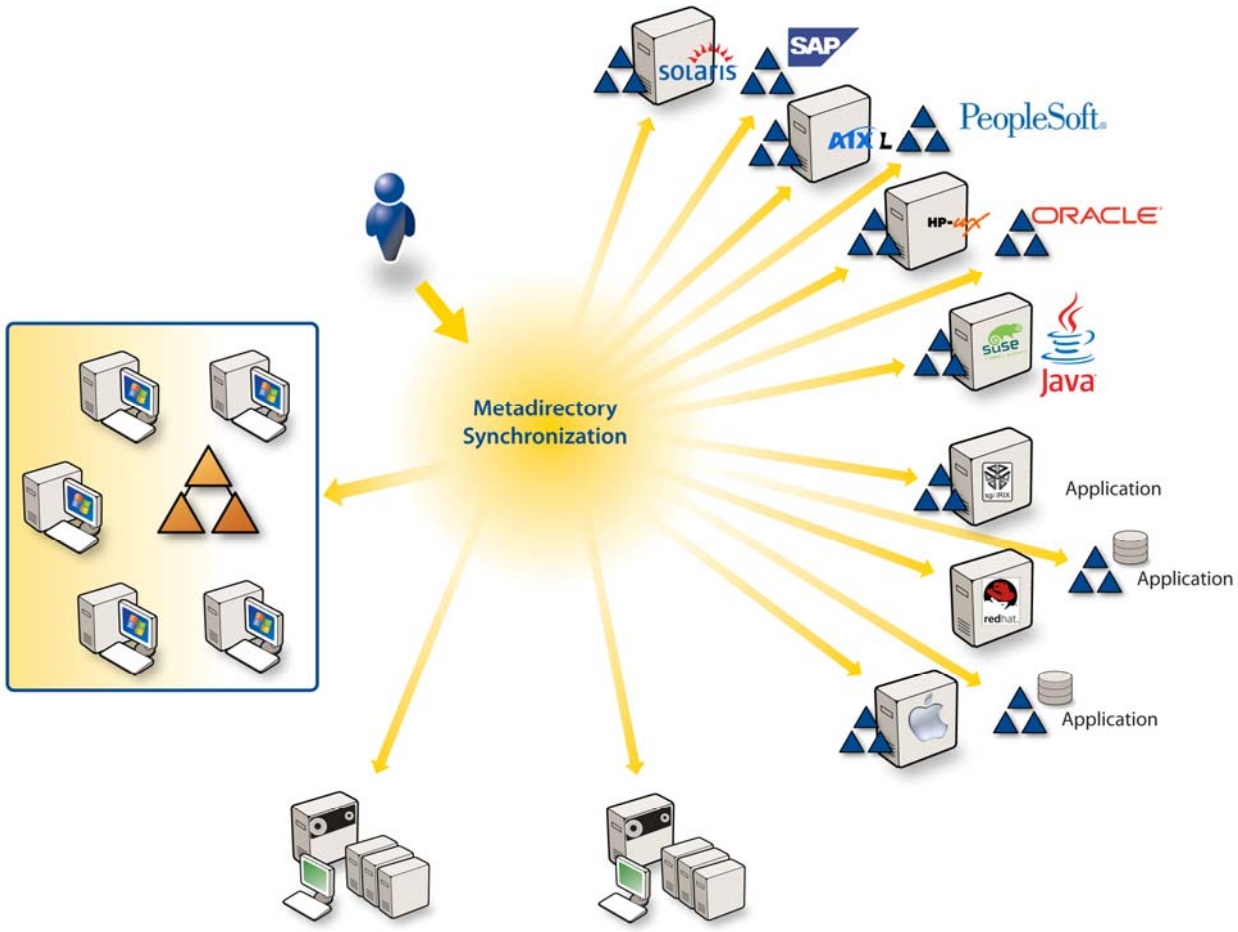
Most organizations have grown in an ad-hoc fashion, preventing them from executing on a consistent identity and access management practices from the start. Therefore, they are left to address challenges as they come up. A system that may have caused no problems when it was procured may now be out of compliance, demanding the organization address a specific challenge with a specific solution. There are several common tactics used to address these problems:

- The security framework approach
- The point solution approach
- The custom approach
- The status quo approach

The Security Framework Approach

One effective approach is to implement a framework around the entire environment to impose structure on the disparate identity infrastructure.

These security frameworks (often called *metadirectories* or *virtual directories*) work by implementing a "master" directory to which all other directories are synchronized. This synchronization requires a custom connector be built and maintained between the application or platform directory and the metadirectory. The connector ensures that actions (such as password reset, provisioning, de-provisioning, or audit) propagate out to the target system or systems.



Metadirectories typically excel as enterprise-wide provisioning agents, but they must address authentication through a "lowest common denominator" approach—all systems and applications can have authentication only as strong as the weakest authentication in the environment. In addition, the security framework approach does not address the underlying problem with heterogeneous environments: the sheer number of identities. Each and every identity—whether associated with a system, application, or platform—still must be maintained and managed. However, the metadirectory does provide a framework for streamlining management.

Because each environment is different, the process of building and integrating the required connectors can be time-consuming and more expensive than the actual purchase of the software. Consequently, only the most progressive or largest organizations have traditionally been candidates for the security framework approach.

The Point Solution Approach

For organizations that cannot or will not adopt the security framework approach, the only option has been to address individual issues as they come up, devising solutions and implementing technologies designed to solve the problem at hand. For example, an organization that needs to implement strong authentication for a critical mainframe system to comply with regulations might select a smart card solution written specifically for the system in question. However, that smart card solution might be specific to that mainframe system, and if strong authentication is later required for another system, an additional solution must be purchased and implemented.

For many organizations, tools optimized for the Active Directory environment can effectively address identity and access management challenges for the largest population of users. Solutions based on Active Directory, including provisioning, self-service password resets, audits, and two-factor authentication, can immediately address many of the demands of compliance, efficiency, and security However, these apply only to Active Directory—not to mainframes, Unix and Linux systems, enterprise applications, or other applications.

Custom-developed Solutions

Another option is the custom development approach. With enough time and effort, organizations can integrate any components. Standards exist and tools are available that enable an organization to integrate its Unix systems with Active Directory. Unfortunately, these projects typically prove to be too complex, time-consuming, and expensive to be viable at large complex organizations. While many organizations have proven that custom solutions can be created in the lab, most quickly opt for a commercially-supported, proven solution from a trusted vendor.

Rely on the Status Quo

The sad reality is that many organizations, when faced with identity and access management challenges, are forced to simply make do with what they have. For these companies, a combination of point solution, custom, and status quo seems to be the only viable option. With enough time and effort, most concerns can be addressed through manual processes, task-specific tools, and point solutions. This approach preserves the underlying inefficiency, does not improve security, and does not address the compliance concerns that are so prevalent in today's computing environment.

The Alternative

What if you could get the best of all of the above solutions? The ideal identity and access management solution would include the:

- Extensive and robust capabilities of the security framework approach
- Targeted functionality of the point solution approach
- Forward-looking innovation of the custom approach
- Cost effectiveness of the status quo approach

The ideal solution would also avoid many of the approaches' shortcomings.

GET TO ONE!

Introducing the Quest One Identity Solution

As we have seen, the root of most identity and access management challenges is the complexity and disparity of the modern heterogeneous enterprise. Eliminating the complexity of myriad identities, authentication practices, roles, policies, and processes is the quickest path to a more efficient, more controlled, and more compliant identity and access management approach. If you have only one identity to manage for each user, the challenge disappears.

Returning to a Homogeneous Environment is Not an Option

How can you achieve a single identify for each user? Clearly not by migrating everything to a single system; the benefits of heterogeneity far outweigh the costs related to managing multiple identities for each user.

What Would a Good Solution Look Like?

The best solution would enable you to retain your diverse systems and applications while enabling you to:

- Consolidate and unify as many diverse identities as possible into an existing directory service
- Eliminate password-related user downtime and inefficiency through single sign-on for all systems, applications, and platforms
- Improve IT and end-user efficiency dramatically by enabling users to help themselves when they have password or other access problems
- Enforce a secure and controlled password policy and strong authentication for all systems and applications
- Improve account management (provisioning and de-provisioning) through automated, rule-based tools based on a ubiquitous, existing identity repository
- Bring identity administration tasks to the help desk rather than to the various platform- and application-specific IT teams
- Lock down sensitive administrative logins across your entire environment
- Authorize web-based access to your internal resources granularly (by remote and mobile employees, partners, and even customers) without additional, cumbersome infrastructure
- Audit your entire environment with a single set of tools and “prove” your compliance, including access control and SOD, before your auditors ask for it
- Speed the implementation and efficiency of your existing security framework, improving your return on investment (ROI)

Simply put: what if you could ***GET TO ONE***—one identity, one point of management, one set of policies, one secure and strong authentication mechanism? What if you could do that without adding infrastructure and without abandoning the diversity that makes your heterogeneous enterprise so valuable in the first place?

Many companies have adopted the "Get to One" strategy in one form or another. New and innovative IT market segments are dedicated solely to unifying diverse identity within existing infrastructure. This strategy is proven to work extremely well in environments with an existing security framework or at organizations with ad-hoc identity administration and diverse identity stores. However, in reality there may be some systems or applications that cannot have their identity subsystems fully unified within the existing infrastructure. Rather than "Get to One," the strategy may be more correctly titled, "Get as Close to One as Possible for as Many Systems as Possible."

> *Aberdeen Group reports:*
>
> *"Best-in-class companies are implementing strategies to reduce the total number of directories in their identity and access management environments; one in five has consolidated to a single authoritative repository for user identities."*[4]

The Quest One Identity Solution

The key to a true "Get to One" strategy is to unify identities completely. Directories are literally consolidated; identity administration automation extends from a single point to all unified systems. And it is done based on infrastructure and a directory that the organization already has.

Quest Software is the only vendor able to deliver the entire "Get to One" strategy. It is implemented through a set of enabling technologies, products, integration, and strategies called the ***Quest One Identity Solution***. Quest One empowers organizations to leverage their existing investments in identity infrastructure—in most cases Microsoft Active Directory—for truly unified identity and access management that crosses platform boundaries. Quest One actually enables organizations to simplify identity and access management. See the appendix at the end of this document for brief discussions of the technologies that make up the Quest One solution.

How it Works

The gold standard for authentication is generally considered to be Kerberos. Of all available commercial directories, only Microsoft Active Directory implements Kerberos on an enterprise scale. Combined in Active Directory with LDAP as the authentication transport protocol, Kerberos delivers single sign-on in the form of one login, one ID, one password, and one credential for seamless and secure access to all Windows resources.

Since the vast majority of organizations house the largest number of user identities in Active Directory, and since Active Directory already provides the best authentication mechanism, it makes sense to implement the “Get to One” strategy by leveraging Active Directory as much as possible. Some questions that may be asked are:

1. Which systems and applications can be unified with Active Directory, and how?
2. What do you do with non-Windows systems that are not equipped to become “one” with Active Directory?
3. Once Active Directory is acting as the authoritative identity repository for the enterprise, how do you optimize its effectiveness?

For some organizations, there is an additional question:

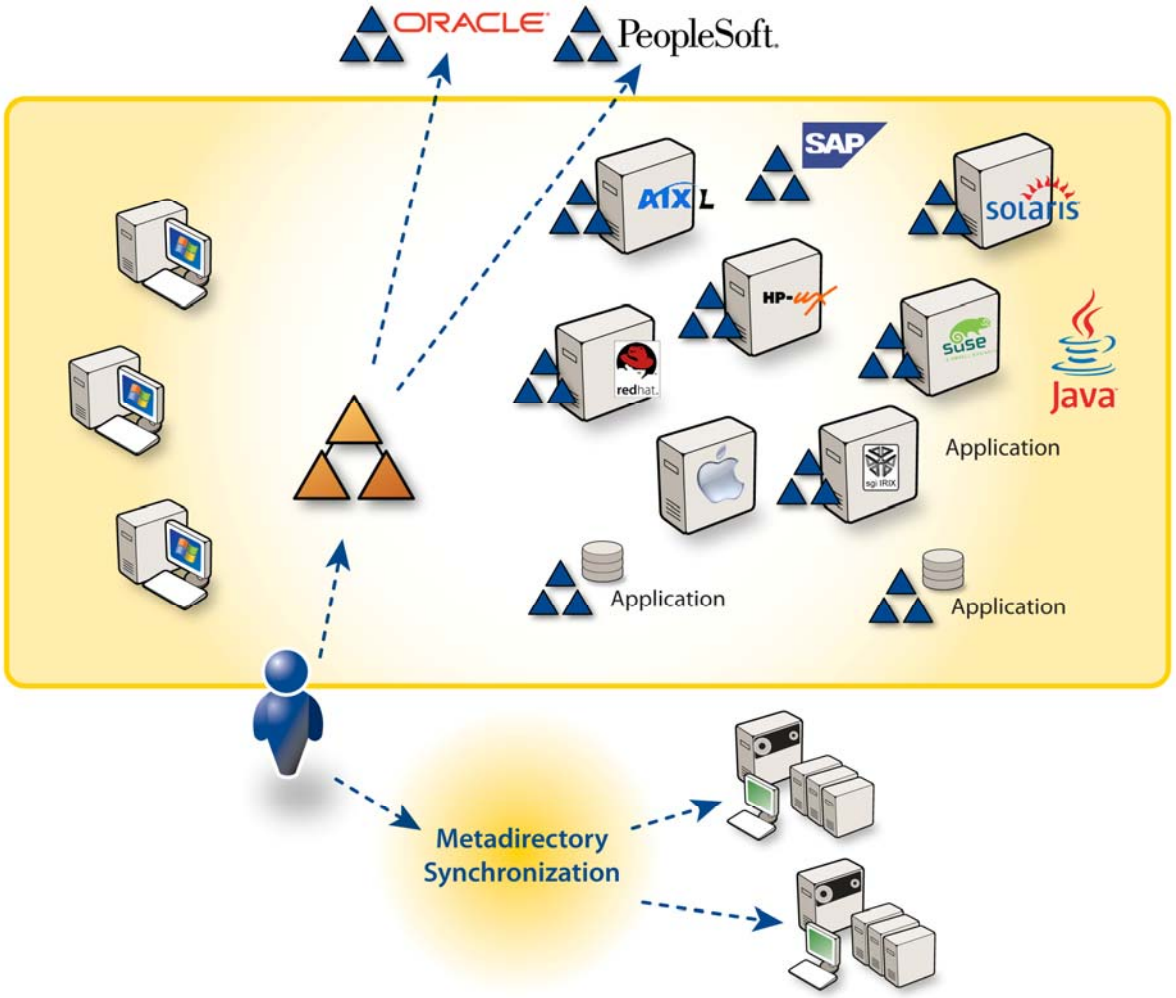
4. Why would I implement the “Get to One” strategy when I already have a security framework?

1. Unifying Non-Windows Systems and Applications with Active Directory

Unifying Systems

Generally, Unix and Linux identities and authentication are some of the most disjointed and difficult to manage in the enterprise. Fortunately the native PAM and NSS identity subsystems of Unix and Linux can be integrated with the Kerberos and LDAP of Active Directory. Quest One technologies make that integration a reality. Quest One enables Unix, Linux, and Mac systems to become “full citizens” in Active Directory, empowering them to act just like Windows clients.

As part of the Active Directory trusted realm, these newly unified systems can achieve Active Directory-based single sign-on. When a user with a Unix account logs into Active Directory, the Kerberos credential (along with any roles, rules, and polices associated with that credential) automatically applies to the Unix login. As a result, many of the inherent shortcomings of Unix identity management (for example NIS, inconsistent password policy, and the need to manually de-provision accounts) are immediately overcome in favor of the more secure and inherently compliant Active Directory.



Immediate benefits of unifying Unix, Linux, and Mac systems with Active Directory include:

CAPABILITY	DESCRIPTION	SECURITY	EFFICIENCY	COMPLIANCE
Kerberos authentication	Extends the natively compliant Kerberos authentication capabilities of Active Directory to Unix, Linux, and Mac systems and many applications; provides single sign-on and directory consolidation.	✓	✓	✓
Password policy	Extends existing Active Directory password policy to Unix, Linux, and Mac systems and applications; enhances non-Windows systems with consistent policy across the enterprise.	✓	✓	✓

CAPABILITY	DESCRIPTION	SECURITY	EFFICIENCY	COMPLIANCE
Access control	Implements consistent access control across all systems based on existing Active Directory roles and policy.	✓		✓
De-provisioning	Provides a common, secure source for all account deactivation based on an existing directory and established identities, roles, rules, and tools.	✓	✓	✓
Strong authentication	Empowers all systems to participate in a single strong authentication infrastructure based on an existing directory and existing identities.	✓		✓
Identity administration	Creates a single point of identity administration (including provisioning, password management, role management, and auditing) for the enterprise without implementing new directories or additional infrastructure.	✓	✓	✓

Unifying Applications

While bringing Unix, Linux, and Mac platforms into Active Directory offers compelling benefits, applications are where most IT effort and user concern are focused. Fortunately Quest One provides many applications with the same level of Active Directory integration that it provides for Unix-based operating systems. Specifically, Quest One provides Active Directory-based single sign-on (and the closely associated reduced sign-on) for:

APPLICATION	QUEST ONE PROVIDES...
SAP	An SAP-certified single sign-on solution that enables an Active Directory login to provide seamless access to SAPgui applications running on Unix or Linux. Quest One also delivers single sign-on for any SAP NetWeaver application.
Siebel	An Active Directory-optimized security adapter that provides reduced sign-on for Siebel running on Unix or Linux.
Java applications	Native Java integration to deliver Kerberos (and thus Active Directory-based single sign-on) to any Java application running on any operating system or web server (including JBoss, Webthority, and WebSphere).
DB2	Integration to enable single sign-on for DB2 instances running on Unix or Linux.
Oracle databases	Integration to enable single sign-on to Oracle databases running on Unix or Linux.

APPLICATION	QUEST ONE PROVIDES…
Kerberos-enabled application	Any non-Windows application that is Kerberos-aware can be easily brought into the Active Directory "trusted realm."
LDAP-aware applications	Any non-Windows application that is LDAP-aware can easily be brought into the Active Directory "trusted realm" through a powerful LDAP proxy.
Applications with an API	Any application with an authentication API (such as GSSAPI) can be integrated with Active Directory for single sign-on.

2. Handling Systems and Application That Can't Be Unified with Active Directory

Some systems cannot be fully unified with Active Directory. Mainframe and midrange systems and some applications do not provide the necessary integration points to become "full citizens" in the ubiquitous directory infrastructure. Although the Quest One approach cannot unify identity and consolidate directories for these systems and applications, "Get to One" can still provide valuable opportunities to simplify identity and access management:

Single sign-on – Quest One includes an enterprise single sign-on offering that enables ANY system or application to participate in a single sign-on scenario. Through login automation, a user's Active Directory (or any LDAP directory) account and login can be replayed on behalf of the user to log in to any application or system. The solution even provides full integration with strong authentication options and the ability to enforce stricter password policy consistently across the entire enterprise. In addition, it can even hide all non-Active Directory logins from the user, further strengthening security and compliance.

Password synchronization – Quest One offers password synchronization capabilities in those cases where integration and enterprise single sign-on are either not feasible or are prohibited. The solution ensures that all non-unified logins use the same username and password as Active Directory. Combined with a powerful self-service password reset solution, this capability addresses some of the password-related concerns of a number of organizations.

In fact, for organizations with existing or planned security framework implementations, the enterprise single sign-on and synchronization capabilities of Quest One may actually be redundant, and the major benefit of the solution is the elimination of underlying complexity and the reduction in the number of directories and identities that must be managed within the security framework.

3. Optimizing Identity Administration

With a much larger cross-section of the enterprise acting as “full citizens” in Active Directory, administering the Active Directory identity becomes more important and should be as efficient as possible. Consolidating to a single Active Directory identity offers the following operational benefits:

- With only one account to provision, re-provision, or de-provision, the traditional challenges of delays and gaps in account termination can be eliminated immediately.
- Provisioning of the Active Directory account (and the newly unified non-Windows accounts) can be initiated through action within an authoritative data source—for example the HR system—and automatically propagated to Active Directory and any security framework that may be implemented.
- Because each user has only one password to manage, a stronger and more consistent password policy can be implemented across the enterprise. It is easier to implement an enterprise-wide self-service password reset solution, and that solution further improves efficiency by freeing up help desk cycles for more important initiatives
- With a single identity and a single authentication mechanism, auditing becomes much easier and can be done more efficiently with a deeper level of knowledge.

Strong Authentication

Many regulations, industry mandates, and best practice frameworks demand stronger authentication than that offered by the traditional username/password login. Quest One provides multi-factor authentication based on Active Directory identity. Specifically, it extends an existing Windows smart card implementation to also include Unix, Linux, and Java systems that have become “full citizens” within Active Directory.

In addition, Quest One provides a powerful one-time password solution that overcomes many of the shortcomings of traditional solutions. It leverages existing Active Directory identity, roles, and rules, eliminating the need to implement an additional directory and manage another set of identities to achieve strong authentication. This approach, which is entirely standards-based, ensures maximum interoperability and seamless, self-paced migration from more cumbersome and expensive solutions. When this powerful solution is integrated with other Quest One components, it adds strong authentication combined with single sign-on, administrative account access, and web-based authorization.

Administrative Accounts

One of the most challenging aspects of identity and access management is the shared administrative account. Most systems, applications, and platforms have a single, all-powerful credential that enables the holder to perform sensitive administrative tasks for these systems. This approach is both necessary and troublesome. Organizations must strike a delicate balance between security and operational efficiency:

- If the credential is given to everyone who might ever need it, a number of administrators may have more rights than necessary—a violation of the segregation of duties compliance principle.
- On the other hand, if the credential is controlled too tightly, getting access when necessary might be difficult, and menial tasks that require administrative credentials must be performed by highly-compensated, busy senior administrators.

Many systems and applications provide the ability to delegate certain administrative tasks based on a user's role and the group he belongs to, while others (for example the Unix root account) are an all-or-nothing proposition. The "Get to One" approach provides alternatives, including implementing a higher level of delegation and control to Windows administrative access and providing a platform for enterprise-wide policy that applies to more administrative accounts.

However, there are cases where the mere unification of identity and consolidation of directories is not enough. For these situations, Quest One offers powerful solutions that integrate with the overall strategy:

Delegating administrative access - Unix provides no native ability to granularly delegate precisely who can do what with the root account. Using Quest One for delegation based on policy, roles, and rules (applicable to any administrative account, not just root), organizations can implement fine-grained control over administrative access and, if desired, fully audit everything that is done with that access.

Issuing the full administrative credential - Even with delegation of access, there are still situations where the full administrative credential can and should be issued. For these scenarios, Quest One offers a powerful, policy-based password vault that automates the process of requesting, approving, issuing, and resetting any elevated privilege account.

Strong authentication - Quest One's administrative access control can be easily augmented through strong authentication—again based on policy—that requires a deeper level of authentication in order to perform certain tasks or to receive the full administrative credential.

Web-based Access

Another identity and access challenge involves granting users, partners, and customers appropriate access to sensitive corporate resources. Web-based access presents significant risk, because it lacks the security of the physical network. But granting web-based access is more important than ever, because of a growing numbers of remote and mobile users, an expanding and more demanding partner community, and the need to automate customer-facing activities.

Quest One provides a solution: access is authorized based on existing identities, roles, rules, and policies. When using Active Directory (or any other identity store) as the authentication mechanism, sensitive data, systems, and applications can be protected from unapproved access, while authorized parties can still be granted access to what they need—nothing more, nothing less. This approach can be further secured by adding strong authentication. It even provides a platform for web single sign-on without additional infrastructure.

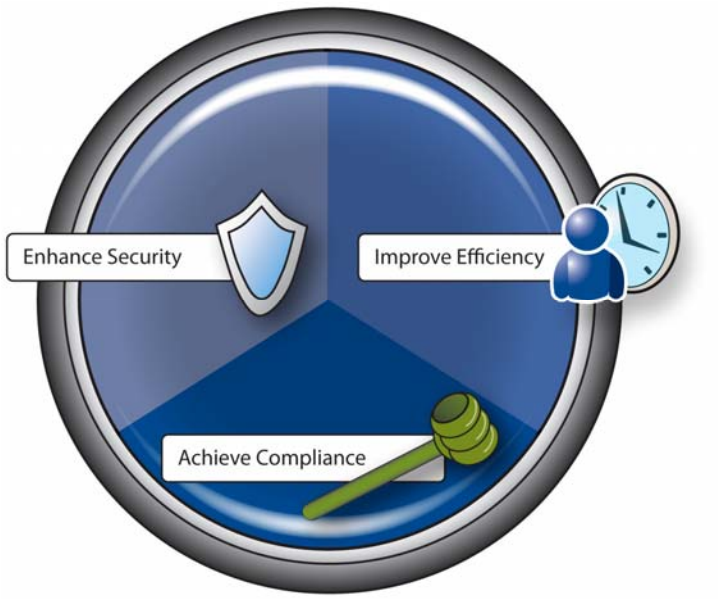
4. Implementing Quest One if You Already Have a Security Framework

For organizations with a security framework, Quest One technology provides the immediate benefit of eliminating the need for individual connectors and custom integration to each Unix or Linux box. For example, in an organization with 1,000 Unix systems, the security framework would require 1,000 connectors (one for each system and each instance of an operating system). However, with Quest One pulling those Unix and Linux systems into Active Directory, the only connector required of the security framework is the one to Active Directory. Since Unix and Linux identities have been entirely eliminated and unified into the more manageable and more secure Active Directory infrastructure, all systems benefit, and a security framework can be implemented more quickly and maintained more easily.

THE BENEFITS OF QUEST ONE

A quick review of the "Get to One" strategy for identity and access management reveals three general benefits:

1. Improving efficiency
2. Enhancing security
3. Achieving compliance



These benefits overlap, and they ebb and flow with the business drivers and environment of the specific organization. Let's review each benefit.

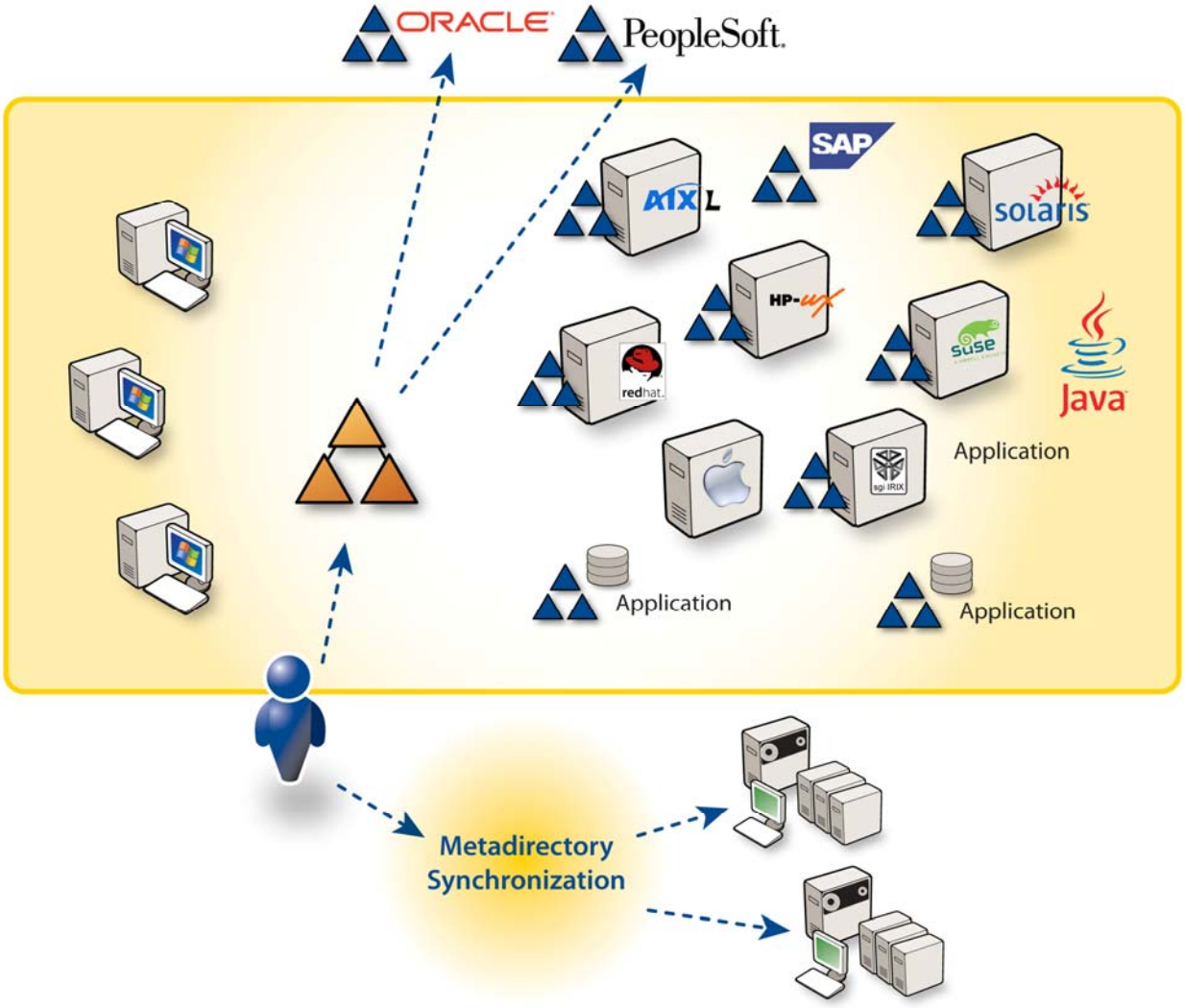
Improving Efficiency

With fewer identities to manage and administer, the "Get to One" approach delivers immediate efficiency improvements and cost savings for both end users and IT staff:

- Single sign-on improves end-user productivity by eliminating the number of times a user must log in and reducing productivity losses due to inability to log in.
- Single sign-on improves IT operations because there are fewer accounts to manage, fewer passwords to reset, and more time to focus on important initiatives.
- Automating identity administration tasks (such as provisioning, password resets, and service enrollment), dramatically reduces the amount of manual process required of IT to manage user identity.

These gains are magnified as more and more identities are consolidated or unified.

The operational benefits of the Quest One approach also apply to organizations with an existing or planned security framework implementation, such as IBM Tivoli, Sun Java Identity Manager, CA Identity Management, or Novell eDirectory. Quest One dramatically increases the efficiency and productivity associated with security frameworks, while reducing their overall complexity. Specifically, a security framework requires unique connectors to every system managed by the framework; the Quest One "Get to One" strategy, dramatically reduces the number of connectors required because many systems can be managed through Active Directory and the single connector between the security framework and Active Directory. At the same time, Active Directory tools can help optimize administration of all user identities, including the newly unified non-Windows identities.



Enhancing Security

Quest One enhances security by providing a more consistent and controllable environment from which security principles can be established and enforced. Systems with limited native security can benefit from the consistent policy, centralized control, and strengthened security provided by Active Directory. For example, with Quest One user and administrative access to systems, applications, data, and resources can be based on a single policy. Existing roles and rules can ensure that only authorized parties get to only the appropriate assets—nothing more, nothing less.

Beyond the authorization aspects of security, the “Get to One” approach also strengthens authentication for systems and applications pulled into Active Directory. Specifically, the Kerberos authentication enjoyed by Windows systems can be extended to Unix, Linux, Mac, and many applications and databases. In addition, traditional multi-factor authentication solutions (including smart cards and one-time password tokens) can also be implemented consistently across the entire, newly-unified enterprise.

Quest One also enhances security in some of the most difficult scenarios, including web-based access and elevated privilege access. These special cases gain dramatic benefit from a unified approach to identity.

Achieving Compliance

Quest One empowers organizations to achieve compliance by unifying previously non-compliant platforms into the inherently compliant Active Directory infrastructure. Consequently, non-Windows access can be tightly controlled based on the roles, rules, and policies that make access in Active Directory compliant. In addition, administrative access can be controlled and segregation of duties can be achieved.

Quest One also enables organizations to implement strong authentication for Windows systems and non-Windows systems alike, immediately delivering core requirements of many regulations.

Quest One provides the capabilities and tools necessary to “prove” compliance. Powerful auditing and reporting tools are available to collect and distribute necessary information from a central identity repository, based on the unified identity in Active Directory. In addition, targeted tools address the auditing needs of specialized situations such as Unix root access, Web-based access, and enterprise single sign-on.

EXAMPLE: HOW QUEST ONE SOLVES REAL-WORLD PROBLEMS

Let's bring the Quest One solution into the real world by considering some of the identity tasks associated with a single user in a mid-sized environment. The table below lists the typical workflow and administrative action for a single employee in a non-unified environment and then compares it to a Quest One environment:

TASK	PREVIOUSLY	QUEST ONE
Employee starts	• Enter in HR • HR contacts IT • IT provisions in AD • IT provisions in SAP • IT provisions in Oracle • IT provisions in Unix (x50) • IT provisions for remote access • IT provisions two-factor authentication (TFA)	• Enter in HR, which automatically provisions to AD, Unix, Linux, SAP, and remote access
Employee logs in	• Once for AD • Once for SAP • Once for Oracle • Once for Unix (x50)	• Single sign-on • One-time self-enrollment for TFA • One-time self-enrollment for enterprise single sign-on (ESSO)
Employee forgets password	• Call help desk for AD • Call IT for Unix • Call IT for Oracle • Call IT for other applications	• Self-service password reset
Employee needs admin rights	• IT issues root (x5) access • Employee retains root access; no control over what employee does with root	• Administrative access delegated based on policy
Employee needs full admin rights	• IT issues password (manual process with no controls) • IT manually resets password after employee is done	• A single automated password vault controls and audits all administrative credential distribution
Employee needs remote access	• Non-secure login • Repeat for each resource	• Secure login based on AD role and protected through reverse proxy • Web single sign-on
Employee changes jobs	• Enter in HR • HR contacts IT • IT re-provisions in AD • IT re-provisions in SAP • IT re-provisions in Oracle • IT re-provisions in Unix (x50) • IT re-provisions for remote access • IT re-provisions TFA	• Change in HR automatically re-provision to AD, Unix, Linux, and all others through security framework integration
IT needs to see what's going on	• Audit AD • Audit Unix (x50) • Audit SAP • Audit Oracle • Can't audit some (root activity, web-based access, etc.)	• Audit AD (and everything pulled into AD) • Keystroke logging of root activities • Audit of remote access • Viewed through a single portal interface

CONCLUSION

Much of the difficulty in identity and access management is rooted in the diversity of the systems, applications, and platforms within organizations. When users have many disparate identities across systems, efficiency, security, and compliance suffer. The Quest One Identity Solution empowers organizations to “Get to One” with their identities and associated tasks. By implementing Quest One, organizations will improve efficiency, enhance security, and achieve compliance.

APPENDIX: QUEST ONE COMPONENTS

ActiveRoles Server – ActiveRoles Server gives you total control of user provisioning and administration for Active Directory. With strictly enforced role-based security, automated group management, change approval, and easy-to-use web interfaces for self-service password management, ActiveRoles Server provides a powerful path to identity compliance.

Defender – Defenders' two-factor authentication ensures that only authorized users are permitted access, whether through VPN for remote access to applications, wireless access points, network operating systems, intranets, extranets, web servers, or applications. Defender works with any OATH-compliant token.

Quest Authentication Services – Quest Authentication Services consolidates Unix, Linux, and Mac identities in Active Directory, extending the benefits of Windows Group Policy to those systems. It also helps migrate NIS environments to Active Directory. Quest Authentication Services also provides single sign-on or reduced sign-on to a large number of applications (such as SAP, Siebel, DB2, Oracle DBs, Samba, PuTTY, and Apache).

Quest Authentication Services Single Sign-on for SAP – Quest Authentication Services integrates Unix and Linux hosts running SAP with Windows-based clients (SAPgui client) through robust, standards-based security. This is the only SAP-certified solution that allows single sign-on for SAP clients through BOTH the SAPgui and the Netweaver web portal.

Quest Single Sign-on for Java – This product provides true Kerberos single sign-on for Java applications and services from Active Directory.

Webthority – Webthority provides secure access to web servers, applications, and content. Webthority simplifies management of access control through role-based authorization and centralized management of user access across heterogeneous web environments. Webthority is able to use a wide range of directories (including Active Directory) as the authentication mechanism.

Privilege Manager for Unix – Privilege Manager for Unix enables you to securely manage and control Unix root access. You can set up policies, delegate responsibilities, and audit all the way down to the keystroke level. Privilege Manager is a "SUDO on steroids" that facilitates management and enhances security.

Password Manager – Password Manager enables end users to reset forgotten passwords securely. This reduces the help desk workload and enables administrators to implement stronger password policies that enhance security. Password Manager supports Windows 2000/2003/2008 Active Directory environments. In conjunction with Quest Authentication Services and InSync, Password Manager allows you to extend self-service password resets to the entire enterprise.

InSync – InSync provides automated password synchronization so users have a single password for all supported systems and applications.

SafeKeeping – SafeKeeping provides a secure, automated mechanism for the request, authorization, release, and change of administrative account credentials.

Enterprise Single Sign-on – Enterprise Single Sign-on can establish single sign-on to any application, system, or platform to reduce help desk costs, increase user satisfaction and productivity, and comply with security policies and corporate governance.

Components and their Benefits

PROJECT	AUTHENTICATION	AUTHORIZATION	ADMINISTRATION	COMPLIANCE
Single Sign-on	Enterprise Single Sign-on InSync Quest Authentication Services Quest Single Sign-on for Java Webthority	NA	ActiveRoles Server Enterprise Single Sign-on Password Manager	Enterprise Single Sign-on InSync Quest Authentication Services Quest Single Sign-on for Java Webthority
Administrative accounts and role-based management	Enterprise Single Sign-on InSync Quest Authentication Services Quest Single Sign-on for Java Webthority	ActiveRoles Server Privilege Manager for Unix Quest Authentication Services SafeKeeping	ActiveRoles Server Privilege Manager for Unix SafeKeeping	ActiveRoles Server Enterprise Single Sign-on InSync Privilege Manager for Unix Quest Authentication Services Quest Single Sign-on for Java SafeKeeping Webthority
Password management	Enterprise Single Sign-on InSync Quest Authentication Services Quest Single Sign-on for Java	ActiveRoles Server Privilege Manager for Unix Quest Authentication Services SafeKeeping	Enterprise Single Sign-on Password Manager	Enterprise Single Sign-on Enterprise Single Sign-on InSync Password Manager Quest Authentication Services Quest Single Sign-on for Java

PROJECT	AUTHENTICATION	AUTHORIZATION	ADMINISTRATION	COMPLIANCE
Audit	InTrust Reporter	Enterprise Single Sign-on InTrust Privilege Manager for Unix Reporter SafeKeeping	ActiveRoles Server	Enterprise Single Sign-on InTrust Privilege Manager for Unix Reporter SafeKeeping
Strong authentication	Defender Enterprise Single Sign-on Quest Authentication Services Quest Single Sign-on for Java	NA	Defender Enterprise Single Sign-on	Defender Enterprise Single Sign-on
Provisioning	NA	NA	ActiveRoles Server Enterprise Single Sign-on	ActiveRoles Server Enterprise Single Sign-on Quest Authentication Services

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 90,000 customers worldwide meet higher expectations for enterprise IT. Quest provides customers with client management as well as server and desktop virtualization solutions through its subsidiaries, ScriptLogic and Vizioncore. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site:	www.quest.com

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

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global Support Guide.pdf

NOTES

[1] "Strong User Authentication: Best –in-Class Performance for Assuring Identities" Aberdeen Group, March 2008.

[2] "Strong User Authentication: Best–in-Class Performance for Assuring Identities," Aberdeen Group, March 2008.

[3] "Provision or Pay: Employee Down Time Costs Companies Millions," Aberdeen Group Research Brief, April 2007.

[4] "Dealing with Directories: Fewer Fuels Faster and More Efficient Operations" Aberdeen Group Research Brief, June 2007