

# Improving the Efficiency and Effectiveness of an Identity and Access Management Framework

---

## **The Narrative of “Company One”**

*Written by  
Jonathan Sander,  
IAM and Security Analyst,  
Quest Software, Inc.*



**Business Brief**

**© 2009 Quest Software, Inc.  
ALL RIGHTS RESERVED.**

This document contains proprietary information, protected by copyright. No part of this document may be reproduced or transmitted for any purpose other than the reader's personal use without the written permission of 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**

Quest, Quest Software, and the Quest Software logo are trademarks and registered trademarks of Quest Software, Inc. in the United States of America and other countries. Other trademarks and registered trademarks used in this document are property of their respective owners.

World Headquarters:  
5 Polaris Way  
Aliso Viejo, CA 92656  
e-mail: [info@quest.com](mailto:info@quest.com)

Please refer to our Web site ([www.quest.com](http://www.quest.com)) for regional and international office information.

Updated—February 4, 2009

# CONTENTS

- INTRODUCTION ..... 1**
- WHAT IS AN IDENTITY AND ACCESS MANAGEMENT PROJECT?  
WHAT DO ORGANIZATIONS NEED?..... 1**
- HOW DO IDENTITY AND ACCESS MANAGEMENT FRAMEWORK  
SOLUTIONS APPROACH THESE ISSUES? ..... 2**
- HOW DOES THE QUEST ONE IDENTITY SOLUTION SIMPLIFY  
THE TYPICAL IDENTITY AND ACCESS MANAGEMENT SOLUTION? ..... 4**
- COMPANY ONE—HAPPILY EVER AFTER..... 6**
- ABOUT QUEST SOFTWARE, INC. .... 7**
  - CONTACTING QUEST SOFTWARE..... 7
  - CONTACTING QUEST SUPPORT..... 7

# INTRODUCTION

The objective of this paper is to review identity and access management challenges, the different solutions/products offered by vendors in order to address them and describe how Quest Software's solutions fit into this broad picture. There will be no attempt to dive into technical details, but there will be some discussion of how the pieces fit together to solve problems. The challenges will be described from the point of view of a typical identity project. The scope of the project will be outlined and then applied to a fictional company. Finally, Quest's solutions will be fit into the picture. It should then be clear where the Quest One Identity Solution fits into any Identity and Access management project.

## WHAT IS AN IDENTITY AND ACCESS MANAGEMENT PROJECT? WHAT DO ORGANIZATIONS NEED?

The phrase "identity and access management" covers a lot of ground. It can be as simple as standardizing information in a directory (like Active Directory) or as complex as managing an entire nation's population information for electronic access to resources. Clearly there is a lot of ground in between those two along with many stops in between. The good news is that you don't need to get a grip on every single aspect in order to understand Quest's role in any project. Too often, people try to figure out what path to take by considering each solution in isolation and seeing how much it can address. Every identity and access management project will require several distinct solutions to fully address all of the issues.

These are the issues typically addressed by identity and access management projects:

1. **Defining what an identity is.** It may be as simple as a distinct entry in a directory or involve data from many different systems that has been consolidated into one or associated by processes.
2. **Rationalizing directories.** This could mean adding infrastructure, such as a metadirectory, or it may involve consolidating many disparate directories into one, depending on the business requirements.
3. **Defining the workflows needed to create, update and delete identity information.** For most, this will mean developing a process for provisioning (bringing a new identity into the company) and de-provisioning (completely removing an identity's rights and access).
4. **Managing the access granted to identities.** Access can range from the ability to get into the network via a VPN to the permissions to edit the price column of one row in a specific database table. All of the rights (or entitlements) can be granted directly via membership in groups, through roles defined in any number of business or IT applications or through other mechanisms.

5. **Managing passwords for all systems.** Help desks and IT administrators are often overrun with password-associated tasks.
6. **Achieving single sign-on.** Often considered the “holy grail” of identity and access management, this is the piece that solves the problems from the point of view of the end users.
7. **Ensuring full audit trails.** Identity and access management projects are often prompted by a compliance driver and the need to tie every audited event to a distinct user.

This list is not complete. Not only could you add to it, you could also break down pieces of the list into smaller issues. For example, you could break down “managing access granted to identities” into role management, managing who has access to administrative rights (privileged access management), who can log into what systems, what contractors are allowed internal e-mail accounts, what groups are allowed to create a new row in a specific table in the HR database and more. This paper broadly examines identity and access management and won’t get into those details. But it is a good idea to remember exactly how complex these issues can become in real projects.

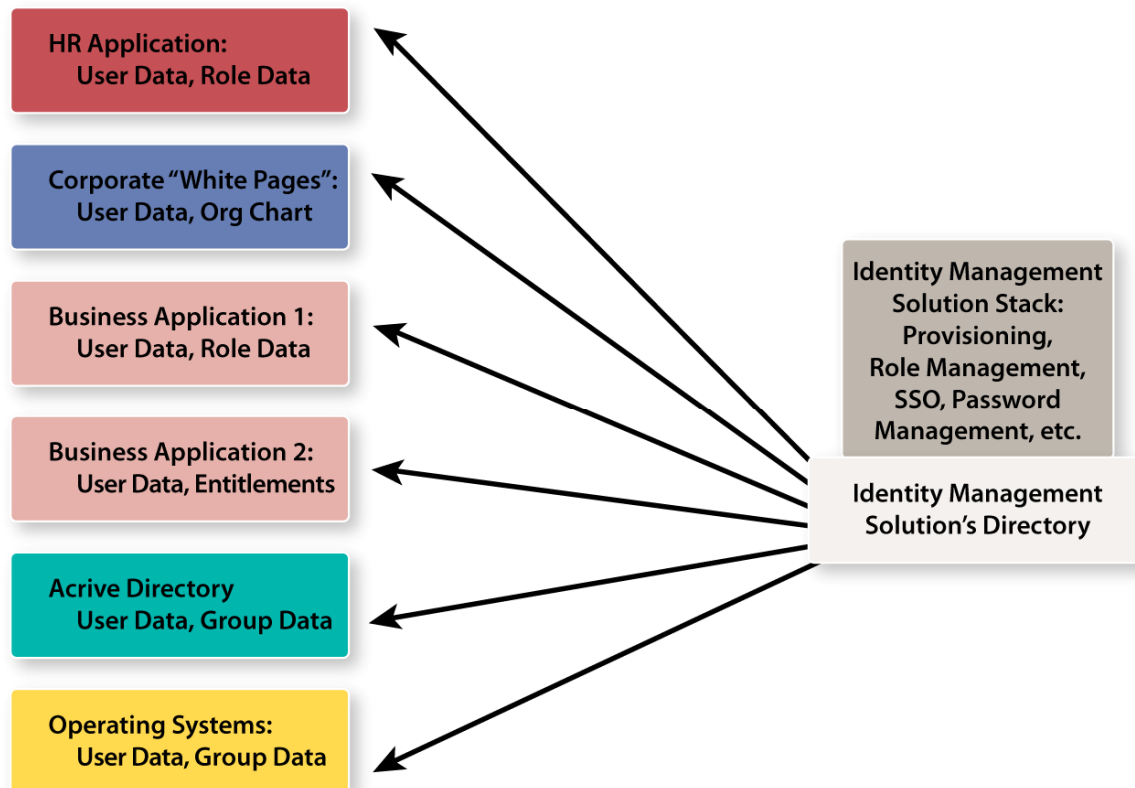
## **HOW DO IDENTITY AND ACCESS MANAGEMENT FRAMEWORK SOLUTIONS APPROACH THESE ISSUES?**

Let’s imagine a real identity management project at a typical company we’ll call Company One. It was prompted by a need to enhance compliance, but gained momentum due to high cost of de-provisioning individuals and assets. It’s fallen to the IT group to sort out the options. They quickly discover they have many pieces of a solution already—maybe too many—including a number of disparate directories, some platform specific identity administration tools, a number of platform and application-specific audit tools, and so on. They also learn that almost every major supplier claims to offer a suite of solutions that will address all of their needs. It’s time for the IT staff to review what the vendors are offering and determine what will fit Company One best.

Vendors who go to market with a full solution for identity management will address all of the issues. They will not only offer tools to help with individual tasks related to identity management issues, but also the fundamental pieces of an Identity infrastructure. The most fundamental piece of any identity management solution is the directory. Directories come in many varieties and from many vendors. We are assuming that Company One is not going to have just one directory, or, for that matter, just one vendor’s directory.

If an organization begins an identity and access management project with only one directory, there are many solutions available to easily address its needs. But Company One not only faces the seven challenges listed above; like most companies, it needs to address them on multiple platforms with a variety of directories from many different vendors.

Directories come in many shapes and sizes and contain data from multiple applications. For example, the data Company One houses in its human resource application can be considered directory data. The company also has additional applications with user data, including a white pages system and customer-facing business applications. Like the vast majority of organizations, Company One uses Microsoft Active Directory for desktop logins connecting to Microsoft Exchange. In addition, other IT services require their own directories, housing user and group data for login. Each of these systems put another directory in place to become the authoritative record of its information.



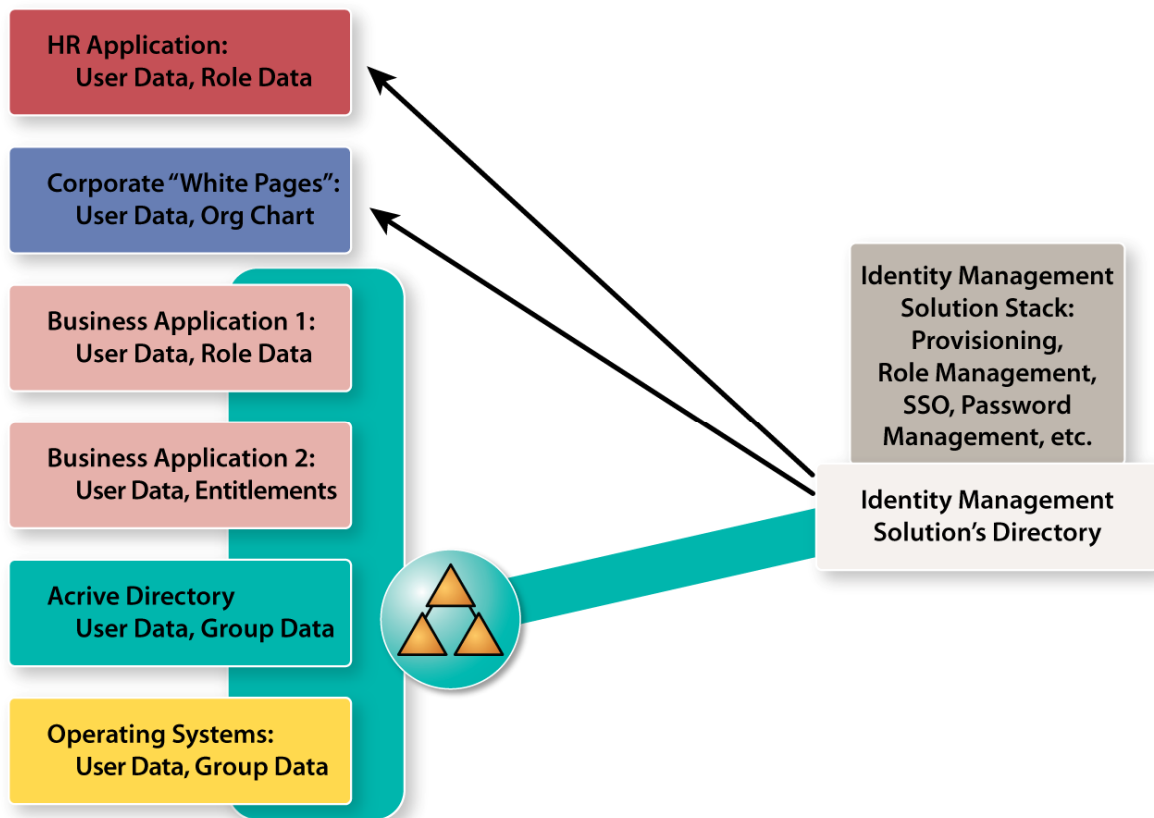
**Figure 1: Typical Identity and Access Management Solution**

If Company One were using a framework (or metadirectory), each system's directory would be populated by connectors that are able to both read and write information to and from the other directories. One new central and authoritative directory would be created; all of the other functions of the solution would be delivered through this directory. Figure 1 shows the identity and access management solution as the hub to all identity data locations. This is a simplified view, but it captures the general approach.

At Company One, the central hub (or metadirectory) would need to connect to more places than depicted in Figure 1. For example, the yellow box, representing operating systems, could potentially correspond to hundreds or thousands of individual Unix or Linux servers. Each of these would require its own connection. Each connector will demand customization, consulting fees and programming. Once established, significant time and effort will be required to maintain this system going forward.

## **HOW DOES THE QUEST ONE IDENTITY SOLUTION SIMPLIFY THE TYPICAL IDENTITY AND ACCESS MANAGEMENT SOLUTION?**

Company One is a customer of Quest Software and uses Quest tools to meet its goals for Active Directory and Exchange management, monitoring and other needs. The IT staff is investigating the Quest One Identity Solution, hoping that it can also help them meet their identity management goals.



**Figure 2: Quest One Identity Solution Simplifies Identity Management**

The only barrier to implementing a framework-type identity management solution is the effort required to allow the central, authoritative directory to talk to all other points where identity information lives. For this reason, Quest concentrates on lessening that effort. Quest's solution allows you to move the identity information, authentication, and authorization associated with many systems, devices, applications and other infrastructure natively into Active Directory. Quest does this by taking advantage of open protocols and standards—such as Kerberos, LDAP, GSSAPI, PAM, NSS, RFC 2307, and others—at the most fundamental levels of the technologies involved. That makes it far simpler than manipulating the various systems from above as connectors must do. With all those pieces tied into Active Directory, the overall number of connectors required drops dramatically. Quest also wraps Active Directory in a layer of heightened interoperability, by putting a proxy layer in place that allows systems to talk to Active Directory via open standards like SPML or via standard means like PowerShell. This will dramatically reduce the effort and infrastructure required to connect to and manipulate this data in Active Directory, as illustrated in figure 2. Since this may increase the sensitivity and volume of work going on in Active Directory, Quest's solution also increases security, ability to delegate, recoverability, availability, performance, and identity administration efficiency of Active Directory with a suite of tools all aimed at giving your Active Directory administrators advanced capabilities in every aspect of operating a powerful Active Directory infrastructure.

However, it's not all about the directory. Company One was also concerned about the productivity of their end users, whose issues can also be just as complex. Some solutions are better than others at trying to simplify their lives. For the solutions that need some help in bringing the "last mile" of a full single sign-on (SSO) solution to every user on every desktop, Quest helps out. First, through the very same integration that brings various systems into Active Directory, Quest One reduces the number of logins needed for any user. All systems hooked into Active Directory are able to use the same user name and password as Active Directory, and many will simply accept the credentials cached when the user signs into their workstation. This eliminates the need for any more work to deliver SSO for those systems and applications. There are also many challenges to integrating thick client, legacy and other desktop applications into a full SSO solution. Quest One includes a comprehensive SSO solution that ties into any existing identity and access management strategy and infrastructure in order to make sure nothing is outside of the reach of SSO. Company One was happy to discover that most Quest One solutions require no coding, scripting or additional infrastructure to support it. It delivers the complete SSO picture without significantly increasing the overall effort.

## **COMPANY ONE—HAPPILY EVER AFTER**

By implementing relevant components of the Quest One Identity Solution, Company One was able to dramatically increase the operating efficiency of its existing identity and access management framework solution. Quest One provided Company One with streamlined administration of identities by carrying out the majority of authentication and administration tasks through its existing Active Directory infrastructure. Consequently, the framework solution, by combining with Quest One, gained a rapid time-to-benefit, was less expensive to implement and maintain, and helped Company One achieve their lofty identity and access management objectives.

## 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. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Visit [www.quest.com](http://www.quest.com) for more information.

## Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)  
Email: [info@quest.com](mailto:info@quest.com)  
Mail: Quest Software, Inc.  
World Headquarters  
5 Polaris Way  
Aliso Viejo, CA 92656  
USA  
Web site: [www.quest.com](http://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](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)