

## *Creating Operational Efficiencies in Identity and Access Management*

---

*Written by  
Don Jones,  
Co-founder of Concentrated Technology  
and Microsoft MVP*



White Paper

**© Copyright Quest® Software, Inc. 2008. All rights reserved.**

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser'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**

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](http://www.quest.com)  
e-mail: [info@quest.com](mailto:info@quest.com)  
U.S. and Canada: 949.754.8000

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

Updated—December, 2008

# CONTENTS

<b>INTRODUCTION</b> .....	<b>4</b>
<b>WHERE ARE YOU SPENDING YOUR MONEY?</b> .....	<b>5</b>
PROVISIONING .....	5
RE-PROVISIONING AND DE-PROVISIONING .....	5
PASSWORD MANAGEMENT.....	6
MULTIPLE DIRECTORIES .....	6
STRONG AUTHENTICATION.....	6
COMPLIANCE .....	7
<b>HOW CAN YOU SAVE MONEY?</b> .....	<b>8</b>
STRATEGIES FOR ELIMINATING REDUNDANCIES .....	8
CONSOLIDATE DIRECTORIES - MAKE ACTIVE DIRECTORY THE CENTER OF YOUR UNIVERSE .....	8
AUTOMATE: OPTIMIZE ACTIVE DIRECTORY PERFORMANCE AND USE.....	9
CENTRALIZE: EXTEND ACTIVE DIRECTORY TO MANAGE MORE.....	9
REDUCE THE NUMBER OF IDENTITIES: INCREASE USER EFFICIENCY THROUGH SINGLE SIGN-ON .....	10
<b>“GET TO ONE” AND SAVE MONEY</b> .....	<b>11</b>
THE SAVINGS ADD UP .....	12
SAVINGS BEYOND MONEY.....	13
<b>SUMMARY</b> .....	<b>15</b>
ABOUT THE AUTHOR .....	15
ABOUT THE QUEST ONE IDENTITY SOLUTION .....	15
<b>ABOUT QUEST SOFTWARE, INC.</b> .....	<b>16</b>
CONTACTING QUEST SOFTWARE .....	16
CONTACTING QUEST SUPPORT .....	16

# INTRODUCTION

Companies spend a fortune—often without realizing it—on identity and access management. If you asked the average IT manager if he'd be willing to hire one person to wash his clothes, another to put them in the dryer, another to fold them, and a fourth to put them in the basket, he would probably look incredulous and ask why a single person couldn't handle all of those tasks. Yet many IT managers preside over a similar assortment of redundancies, spending money to maintain disparate systems that all perform essentially the same task in very slightly different ways.

Many efficiencies can be realized by understanding where money is being spent unnecessarily. As with many IT challenges, additional tools or solutions may be required to achieve those efficiencies, so in addition to understanding where improvements can be made, we also need to discuss how those improvements can be funded.

# WHERE ARE YOU SPENDING YOUR MONEY?

As IT environments grow, companies are acquired and merged and management regimes change, the IT infrastructure often accumulates a startling amount of redundancy. It also tends to accumulate an unhealthy amount of manual labor—despite that fact that computers are the very things that are supposed to be *reducing* manual labor. Getting different systems properly configured and communicating is often seen as a one-time task, when in fact it can turn into an ongoing process that distracts IT resources and costs the organization more than necessary. In the next several sections, we'll look at some of the places where you may be spending your money unnecessarily. These are the areas ripe for a more efficient approach.

## Provisioning

*Provisioning* is the process of creating a new employee's digital identity within the organization and assigning access permissions to that identity. Simply put, it's the act of creating a directory account and making sure the account can access everything the user needs for day-to-day tasks. Provisioning may also include creating a messaging account (such as an Exchange Server mailbox) and other "set-up" tasks.

Unfortunately, organizations tend to have to provision a *lot* of different things: HR management systems, ERP systems, various directories that control access to different types of resources, phone systems, and more. While some of these steps, such as provisioning the phone system, might be unavoidably separate, others represent a frustrating redundancy. If you're already setting up user accounts in Active Directory, why do you also have to set up user accounts in eight other places? Every set-up consumes time, creates another point that has to be audited for compliance requirements as well as another opportunity for human error. This results in *more* time and money spent correcting any errors.

## Re-Provisioning and De-Provisioning

Once a user's identity and access is set up, the work doesn't stop. As users move through the organization because of promotions, re-organizations or lateral moves, their identities must be constantly adjusted to match their new responsibilities. Users promoted into management positions may need an account added to the ERP system, while users who move out of sales may need to have their CRM system account turned off. Access permissions on files, folders, e-mail accounts, instant messaging accounts, HR systems, databases, and more all need to be constantly updated, which creates ample opportunity for more manual labor, simple human error, and user downtime.

When a user leaves the organization, work can actually increase. Not only do administrators need to track down and disable each and every identity across the enterprise, they also need to determine who should be assigned replacement access to the former employee's resources, and then spend time reconfiguring those resources accordingly. Any administrator will be happy to

tell you how much time all of this identity and access management takes. Any compliance auditor can tell you how difficult it is to properly track all of this “churn,” and how upset the authorities get when you *don't* properly track it all.

In the end, it comes down to a lot of time and money being spent managing nearly identical tasks separately on different platforms on a continuous basis.

## Password Management

With all these identities floating around, it's no wonder that users lose track of their passwords, lock out an account, and end up on the phone with the help desk to sort things out. In a 2005 report, analysts estimated that password problems consume 25%-40% of help desk call volume. Some studies estimate that help desk calls related to password management cost \$10 to \$31 per call, and that an organization can reasonably expect every user to have an average of 1.5 issues per year. That's expensive. It's also a lot of volume that ties up help desk resources that could be put to better use elsewhere. In fact, some organizations aren't able to staff their help desks to the level needed to handle all of the password problems in addition to the other calls that come in. This means that expensive higher-end administrators may end up handling the spillover—not the best use of the human IT investment.

## Multiple Directories

The use of multiple directories creates much of the expense and labor involved in provisioning-related tasks, and each directory has its own management overhead, including: backups, recovery operations, performance management, software patching, security configurations and auditing. Nearly every directory will require roughly the same administrative tasks on an ongoing basis; if it takes one administrator five hours a week to maintain a single directory, it will take that administrator about 20 hours to maintain four directories. By studying what those directories are supporting in order to find ways to get rid of some of them, you can realize significant savings.

## Strong Authentication

Many organizations use strong authentication to improve security. *Strong authentication* generally refers to multi-factor authentication, with two-factor authentication as the most common. While these schemes may involve biometrics or other more exotic techniques, one of the most common two-factor authentication systems is a hardware or software token combined with a PIN or password. These systems greatly reduce the possibility of an attacker or other unauthorized individual gaining access to IT resources.

Unfortunately, these systems often represent yet another directory that needs to be provisioned, maintained, de-provisioned, audited, and managed. This means more overhead for the IT staff and additional help desk calls. Ideally, pulling these multi-factor authentication systems into an existing

directory would help smooth and streamline operations, as well as save money.

## Compliance

The biggest burden faced by many IT organizations today is dealing with the increasing number of industry and legislative requirements that the industry collectively refers to as *compliance*. Compliance consists of very broad and complex security requirements, including many that involve tracking and auditing the current and historical state of systems, their availability and change control.

Compliance takes a lot of effort. And the more systems you have, the harder compliance becomes: every management point needs to be properly configured, audited, backed up, and managed each day. The more directories and IT resources you have, the more compliance will cost. And some systems, particularly legacy ones, are more difficult to make compliant than their more modern counterparts—for example, Unix's NIS is more of a challenge than Window's Active Directory.

Unfortunately, compliance isn't optional. You can't just decide not to do it, and so you're forced to pay the price of maintaining compliance across your *entire* IT infrastructure—multiple directories, many resources, and all.

# HOW CAN YOU SAVE MONEY?

## Strategies for Eliminating Redundancies

Multiple directories entail multiple redundancies, which mean there's room to save by eliminating those redundancies. Focus on the following:

- Eliminate redundant directories through consolidation, preferably around a directory you already have as opposed to creating yet another directory to manage all your current directories.
- Reduce the number of identities in the environment through directory consolidation. Use single sign-on or automation to reduce the time and resources required to manage those identities.
- Improve consistency by eliminating platform- and application-specific tools. Instead use higher-level, business-focused tools that can manage multiple underlying systems.
- Eliminate redundancy in access management, a key part of the overall provisioning process, by using policy-based management tools that use business-level policies to automate management tasks.
- Reduce and eliminate manual tasks by relying on automation, and offer self-service options for tasks that would otherwise consume IT resources.

Quest believes that a simplified, more business-focused environment can offer significant savings. The key is in understanding what capabilities the technology industry currently offers for achieving these goals. A good approach can take advantage of several possible savings points, including consolidating directories and automating, centralizing and reducing the number of identities.

## Consolidate Directories - Make Active Directory the Center of Your Universe

Microsoft's Active Directory is already an important part of your enterprise. Whether you're using it to support an Exchange Server messaging infrastructure, to secure access to Windows client computers, or to secure access to file and print servers, everyone in your organization already has an Active Directory identity. Active Directory is an actively-developed, mature product that has a long life ahead of it. Why not eliminate other less-capable directories in favor of Active Directory? This would help eliminate the redundant effort associated with managing multiple directories and can result in significant savings.

Of course, it's not enough just to get rid of a directory. You also need to continue to support the systems that relied on it, and consolidate any of its identities by associating them with their corresponding Active Directory accounts.

## **Automate: Optimize Active Directory Performance and Use**

Active Directory itself can consume significant management time because its native toolset tries to present a common administrative scenario for all environments. By eliminating this time-consuming and inefficient manual management, you can optimize Active Directory's usage and realize significant savings.

Switch to top-level, role-based management that aligns access control and identity management to business needs, and then automate it so that it requires less effort. By automating user provisioning, re-provisioning, and de-provisioning, you can combine identity and access management into a single, business-driven task that is initiated, completed, and maintained automatically across the enterprise.

Eliminating manually-performed tasks for ongoing maintenance is another key. For example, help desk calls dealing with account issues such as account lockouts and password resets result in significant help desk expenses (up to \$31 per incident, by an analyst estimate) and user downtime. Implementing self-service systems that allow users to resolve these incidents on their own can reduce costs to just a couple of dollars per incident.

Increasing the manageability (and thus the security and compliance) of Active Directory can also save time and money, and result in a more reliable directory infrastructure. You can achieve this through the use of more granular and automated management capabilities not provided by the native Active Directory toolset.

## **Centralize: Extend Active Directory to Manage More**

By investing in Active Directory, streamlining its usage, and providing self-service options to reduce support costs, you can make Active Directory a better-performing, money-saving part of the enterprise. Once you've done that, why not extend those savings even further by using Active Directory to eliminate redundant directories and identities in parallel technologies and improve security?

Active Directory can be extended to provide authentication for users of Unix, Linux, and Mac systems, eliminating platform-specific directories currently used to support those platforms. Group Policy configuration control can also be extended to Unix, Linux, and Mac, bringing server and client configurations under a centralized directory. Single sign-on can extend Active Directory for key enterprise applications such as Java applications, Siebel, SAP, DB2, and Oracle databases, eliminating the management overhead of maintaining individual identities in those systems.

Multi-factor authentication (such as hardware tokens) can vastly improve security within the environment, and can be implemented as an extension of Active Directory itself. This helps you better meet many common compliance requirements without the addition of another directory. If you're already using two-factor authentication, integrating it with Active Directory can reduce management overhead while maintaining the benefits.

The idea is to use every feature that Active Directory offers and extend it uniformly across the enterprise.

## **Reduce the Number of Identities: Increase User Efficiency through Single Sign-On**

Single sign-on, which we've already mentioned, is one of the most common goals of IT managers, yet seems to be one of the most difficult IT goals to achieve. It *is* achievable with the right combination of tools and know-how, especially when based in Active Directory. With single sign-on, users have to remember fewer identities; this means they'll be more productive because they'll *remember* their passwords. Single sign-on helps administrators work more efficiently as well; they are managing fewer identities in fewer places.

# “GET TO ONE” AND SAVE MONEY

Quest’s vision of saving money through better use of Active Directory is best expressed by the **Quest One Identity Solution**. Its philosophy: One Identity, One Point of Management.

The idea is simple: make Active Directory the center of your identity management universe, and extend Active Directory to as many systems and platforms as possible. This creates a single point of management for identities across the enterprise, eliminates redundant management efforts and saves you a great deal of time. It also helps users become more efficient in their day-to-day tasks by giving them single sign-on; fewer identities for users means fewer mistakes, fewer help desk calls, and better productivity. Self-service tools that allow users to partially manage their own identities (such as unlocking their own passwords when needed) increase your savings by further reducing help desk calls and keeping your users on the job.

The Quest One Identity Solution approach allows you to:

- **Improve efficiency** by managing fewer identities in fewer places, and by improving end-user productivity by giving users fewer identities to deal with. Both users and administrators spend less time focused on identity management and more time being productive.
- **Enhance security** by providing a more consistent and controllable environment from which security principles can be established and enforced. Extend Active Directory’s consistent policies, centralized controls, and stronger security to systems with limited native security, and enhance security in difficult scenarios such as access using Web-based elevated privileges.
- **Achieve compliance** by unifying previously non-compliant platforms into the inherently compliance Active Directory infrastructure. Non-Windows access can be tightly controlled based on the roles, rules, and policies that make access in Active Directory compliant. Active Directory itself can be made easier to audit and provisioned with strong authentication, immediately delivering the core requirements of many compliance scenarios.

Quest believes that you can achieve these benefits by addressing four distinct areas within the enterprise:

- **Authentication:** the means by which users identify themselves to IT systems and applications.

More broadly, authentication is part of identity management, and the Quest One philosophy is to manage identities and authentication in fewer places, using a consolidated directory that serves the entire enterprise, not just a single platform.

- **Authorization:** the process that determines what resources users will be able to access, also known as *access control*.

The Quest One approach is to manage authorization in as few places as possible, using techniques that foster a business-centric view rather than a technological view.

- **Administration:** the act of managing authentication and authorization.

Quest believes that administration tends to be overly manual, meaning administrators work too hard to implement configurations, maintain them, and audit them. Significant savings and better consistency can be achieved through automation.

- **Compliance:** the ability to *prove* that your enterprise meets applicable industry and regulatory requirements.

This consists not only of auditing, but also of automated configuration control and remediation. This helps to ensure that the proper configurations are in place at all times and proves that they *been* in place now and in the past.

## The Savings Add Up

It's always difficult to cite exact savings in IT projects because every organization is different. But it is possible to take a couple of common scenarios, provide background numbers, and get a good idea of the amount of savings that you can realize.

### Example: Separate Directories

Let's consider an organization currently managing five directories: an Active Directory domain, an NIS domain for Unix and Linux systems, a home-grown Java application with its corresponding authentication mechanism, SAP for ERP, and a legacy mainframe system. This is a common situation for larger companies that have been acquired or merged with others, causing them to accumulate a variety of IT solutions that are more or less standalone.

Suppose that the organization adds 2,500 new users each year, loses 1,500 employees each year, and moves 4,000 employees due to promotions, reorganizations and lateral changes. That's 8,000 identity changes in total, across five directories, for a total of 40,000 directory changes. Suppose also that it takes an administrator 20 minutes to provision a new identity in each directory (including managing the resource access associated with the directory identity), 20 minutes to change an identity (which often involves changes to access controls), and 60 minutes to de-provision an identity. These times are actually quite conservative; field experience suggests that some organizations may require much longer for these tasks.

That adds up to more than one million minutes of work per year, or about 18,000 hours—essentially a full-time job for nine administrators, with no holidays or vacations. For administrators being paid \$95,000 per year (including benefits and employer taxes), that's an expense of \$855,000 per year. Keep in mind that this scenario is greatly simplified simply to illustrate a point of scale.

### Example: Directory Consolidation

The Quest One approach consolidates the five directories into one directory—Active Directory. It also implements automation for access control, significantly reducing the amount of time required to manage access permissions across these various systems. Now directory management occurs in one place, and access management times are much shorter. The organization might find it takes an administrator only 10 minutes to provision a new user or to make changes on an existing user, and perhaps another 10 minutes to de-provision a user.

The company in our example above had 40,000 directory changes a year, at an annual cost of \$855,000. With Quest One, those 40,000 changes translate to 77,000 minutes of work per year, or just over 22 hours per week for an entire year, for a single administrator, at an expense of roughly \$57,000. In other words, Quest One provides a potential savings of nearly \$800,000 per year:

\$855,000 per year without directory consolidation  
- \$ 57,000 per year with Quest One

**Potential savings: \$798,000 per year**

Much of the savings is realized simply by having fewer points of management thanks to the directory consolidation.

Again, this is obviously a simplified example, but it illustrates the scale of the savings that can be achieved by reducing the number of management points in the enterprise, and in automating much of the remaining management which would otherwise be manual and time-consuming.

### **Self-Service Password Management**

This is an area that's almost an instant "win" in terms of saving money. The average help desk spends almost half of its time dealing with password-related issues, including as password resets and account unlocks. Let's assume that the cost of each help desk call in a specific organization is about \$20 (a very conservative estimate). This reflects the amount of time it takes to completely resolve each call, the cost of supporting infrastructure (phone lines, help desk computers, etc.) and other associated costs. This also reflects the cost of the user's downtime while waiting for the issue to be resolved.

Self-service password management solutions, which permit users to securely and safely unlock their own accounts and reset their own passwords, eliminate most of these calls. Conservative estimates suggest that a company of 1,000 users that deals with 1,500 password-related issues per year will save about \$26,000 per year, less the cost of implementing the self-service solution. This savings comes from significantly reducing the user's downtime and by dramatically reducing the amount of help desk calls relating to passwords.

## **Savings Beyond Money**

Quest One not only saves money, but offers other benefits as well.

### **Reliability and Productivity**

First, Quest One can increase the reliability of your entire IT infrastructure, improving up-time and increasing user productivity. When users aren't waiting for IT assets to become available, those users are doing what they do best: contributing to the organization by remaining productive.

### **Administrator Efficiency**

The right approach can also make your administrators more efficient and effective. Rather than focusing on day-to-day configurations, which are largely repetitive and uninteresting, administrators can focus on their core responsibilities, such as managing overall systems performance, handling big-picture technology issues, and maintaining the overall environment. This frees up administrator resources for new projects, allowing you to implement new technologies and products that benefit the company *without* increasing headcount or relying solely on outside consultants.

### **Easier Compliance**

Another benefit is the ability to more easily meet your compliance requirements - managing fewer directories and implementing centralized, secure auditing and reporting makes achieving compliance much easier.

### **Increased Security**

Finally, you'll also realize significant improvements to your organization's IT security—a common result of achieving and maintaining compliance. With fewer management points to secure and automated security controls, you'll have better visibility into your system and be better able to align its security to specific business needs.

### **Finding the Budget to Save Money**

Finding the budget to improve Active Directory operations is difficult in today's business environment. No matter how you argue for improved stability and control, it's difficult for businesses to allocate funds to something that doesn't seem to contribute directly to the business' bottom-line profitability. It's also difficult to find the budget for identity and access management; while improved management capabilities will certainly save money by making administrators more efficient, it's difficult to point to concrete bottom-line savings.

It may be necessary for you to refocus your proposal. We've already examined the ways in which improved Active Directory management and identity and access management can create a better compliance posture for the organization, making it easier to achieve and maintain compliance throughout the enterprise. Unlike management and operations, compliance is something most organizations find it easy to budget for, since compliance isn't optional. It may be simpler to pursue improvements to Active Directory and identity and access management by focusing on the compliance benefits. Your organization may be more willing to implement these upgrades and solutions in order to help you more easily meet and maintain your compliance requirements; the management and operational improvements will come along as side benefits.

# SUMMARY

## About the Author

Don Jones is a co-founder of Concentrated Technology (ConcentratedTech.com). His consulting practice specializes in making the connection between technology and business, helping businesses realize more value from their IT investment, and helping IT align more closely to business needs and values.

Don is also a Microsoft Most Valuable Professional Award recipient and the author of more than thirty books on information technology. He has been an IT journalist for more than eight years, and is currently a Contributing Editor for *Microsoft TechNet Magazine*. He is also a sought-after speaker at industry conferences and symposia, including Connections conferences, Microsoft TechEd, and TechMentor Events.

## About the Quest One Identity Solution

The Quest One Identity Solution increases efficiency, enhances security, and enables compliance by reducing identity management complexity, automating key identity administration tasks, and building on existing investments. Quest One helps with single sign-on, provisioning, password management, role management, strong authentication, audit, and directory consolidation with your existing identity infrastructure.

# 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 100,000 customers worldwide meet higher expectations for enterprise IT. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Quest Software can be found in offices around the globe and at [www.quest.com](http://www.quest.com).

## 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_Support_Guide.pdf)