QUEST SOFTWARE
Smart Systems Management

Managing Macs in a Windows World and Integrating them into an AD-based Network

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

WHITE PAPER

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: **legal@quest.com**

Trademarks

Updated—November 2009

Contents

Introduction

Apple's Mac computers are growing in popularity in today's corporate environments for many reasons. Sometimes Macs are in demand simply because they're not Microsoft. Some users have a perception that Macs are safer and more stable, resulting in demand—often from influential user communities like executives—for more Macs. In other cases, Macs are chosen because they're better for specific tasks, such as design and multimedia work, or they are chosen for user populations who are most comfortable with Mac-based tools. Some organizations, such as the US Army, are adding more Macs simply to increase the diversity of their computing base and to reduce the scope of damage from a single attack.

The increasing number of Macs in the IT environment creates new challenges for IT staffs, who need to maintain the same level of security and manageability on Macs as on their Windows systems. Allowing Macs to operate as standalone pockets of individualism is no longer acceptable: today's Macs need to be first-class citizens within larger IT initiatives such as identity management, security, compliance, and policy-based management.

Apple has taken a few steps to make Macs as enterprise-friendly as Windows is today. On the surface, Macs and Windows seem to enjoy a great deal of parity in terms of business functionality:

- Both can run versions of Microsoft Office.
- Both can be centrally configured by policy-based management: Group Policy for Windows, and Apple Workgroup Manager for Macs.
- Both can work with Exchange Server, using Microsoft Outlook on Windows, and Microsoft Entourage on Macs.
- Both can authenticate to Active Directory.
- Both can share files and printers using variants of the Server Message Blocks (SMB) protocol.

When you dig deeper, however, things aren't quite equal between the two platforms. This paper outlines the two significant challenges to making Macs a first-class network citizen, and a Quest solution that can help.

The Challenges Facing Macs

Application-specific issues aside, Macs face two primary challenges when it comes to participating in a Windows-based network: authentication and policy-based management.

Authentication

While Mac computers can be configured to authenticate users to Active Directory (AD) by obtaining and managing Kerberos tickets in much the same way Windows clients do, Mac computers themselves don't typically authenticate to the directory. This creates a disconnect between the management capabilities between Windows and Macs, and can significantly impact the ability to create a single sign-on environment. Mac computers may have to authenticate multiple times in multiple-domain environments, and maintain their own local user accounts used to secure resources on the Mac computer.

Both first- and third-party solutions exist to better integrate Macs into AD. Utilities from Apple, included in Mac OS 10.5 and later, focus primarily on user authentication. Many third-party utilities also focus entirely on authentication and don't extend many AD benefits to Macs. For example, they may not support access control or password policy; in some cases, they may not even permit users to change domain passwords from a Mac. They also may not work in complex, multi-forest environments.

Some third-party solutions do provide broader capabilities than authentication, but are often just as Mac-specific as Apple's utilities. If Macs are your only non-Windows platforms, these third-party solutions may be acceptable. However, if you also want to integrate Unix and Linux systems, then having a single "non-Windows integration system" that accepts all of these types of computers can significantly reduce management overhead and cost.

The importance of achieving a single sign-on capability cannot be overemphasized. Maintaining a single credential for each user vastly simplifies not only identity management (which in turn simplifies overall security, compliance, and maintenance), but also simplifies users' lives, helps prevent forgotten passwords (and the resulting help desk calls), and improves both user productivity and satisfaction.

Policy-based Management

Microsoft's solution for policy-based management is Group Policy, an integrated part of Active Directory that requires significant client-side support from within the Windows operating system. Apple offers a parallel technology called Apple Workgroup Manager; it requires at least one Mac OS X Server-based computer and requires Mac clients to authenticate to that server in order to obtain policy information.

Neither of these systems natively addresses Linux or Unix computers, so you may wind up maintaining two distinct policy-based management infrastructures—one for Windows and one for Mac—and still not address your entire computing base.

In addition, Apple and Microsoft handle different settings in different ways, so your two-policy systems will never be exactly equal. And simply having two parallel systems opens significant room for error and inconsistency; for example, it is easy to make a change on one system but forget to make the corresponding change in the other system. These errors and inconsistencies can negatively impact security, compliance and stability.

Of the two systems, Group Policy is definitely superior. It is a tiered system that ties to existing AD hierarchies and groups, and many first- and third-party systems extend Group Policy to include versioning, change control, and other manageability benefits. Moreover, Windows environments natively have AD, making Group Policy a free side benefit, but environments with Mac clients do not necessarily have a Mac OS X Server computer. This means additional effort is required to implement Workgroup Manager.

What's needed is a way to extend AD's Group Policy features to the Mac and, ideally, to *all* computers—Unix and Linux as well as Mac. This will enable customers to gain additional benefits from their existing technology investment and enjoy a single policy-based management system.

The Mac Solution: Quest Authentication Services

Quest Authentication Services uses patented technology to extend Active Directory-based authentication to non-Windows computers, including Mac, Unix, and Linux machines. It offers several major features that apply specifically to Macs in a Windows environment:

- Kerberos-based single sign-on, which allows Macs to authenticate as easily as Windows computers do
- Access control, which simplifies both security and compliance by bringing a scalable access control system to all computers in the environment
- Integration with Microsoft's Active Directory Users and Computers console, giving administrators a single place to configure a single infrastructure
- AD extended to Mac, Linux, and Unix computers
- Group Policy extended to Mac, Linux, and Unix computers

Mac Authentication

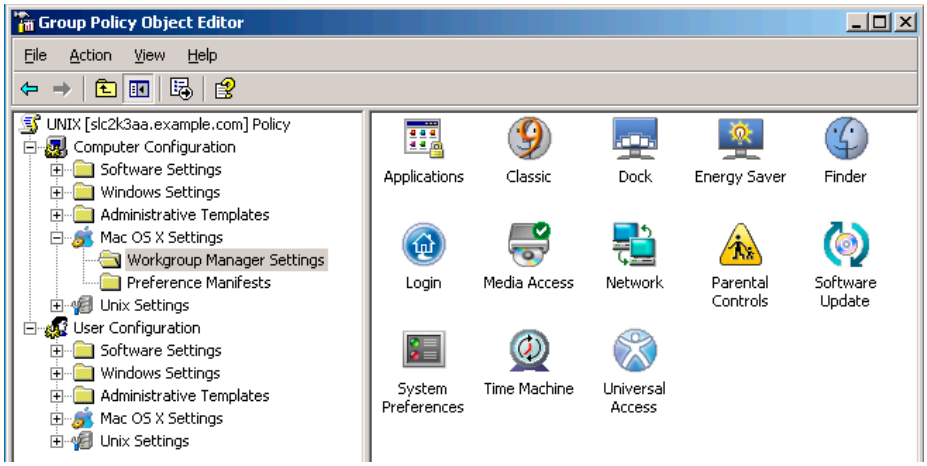
When AD was introduced in 2000, its use of the industry-standard Kerberos authentication protocol opened the door for wider interoperability, making authentication essentially a commodity, even when authenticating to Macs.

Quest Authentication Services ensures that Macs—and Unix and Linux computers—can authenticate seamlessly to AD, maintain computer accounts in AD, and essentially behave just like Windows computers when it comes to your domains and forests. Quest Authentication Services is the most robust and scalable solution of its kind available today, capable of supporting any size Active Directory environment.

Quest Authentication Services can also provide single sign-on in environments that use key enterprise applications, including SAP, Siebel, Java, Oracle databases and DB2.

Mac Group Policy

The ability to extend Windows Group Policy to Mac computers is extremely beneficial: it creates a policy-based environment that's more secure, stable, compliant and easy to manage. When fully-integrated with the Microsoft Group Policy Management Console (GPMC), Quest Authentication Services Group Policy for Mac makes "Mac Group Policy" as straightforward as "regular" Group Policy. Its purpose-built interface is clean, efficient, and intuitive and supports almost all of the Mac's preferences and settings.



You can set preferences and policies, including the following:

- **Finder** – Mac's equivalent of Windows Explorer, using preferences to configure the computer's look, feel, and general behavior
- **Dock** – Mac's version of the Windows Taskbar for configuring Dock behavior, applications, and more
- **Login** – Controls the systems that Mac authenticates to
- **Classic** – Mac's OS 9-compatible system that controls major system preferences, accessibility to the Classic subsystem, etc.
- **Universal Access** – Mac's accessibility subsystem that controls accessibility features and availability
- **Network** –Controls settings such as DHCP, default networks, wireless networking, and more
- **Energy Saver** – Controls Mac sleep settings, power savings settings, and more
- **Parental Controls** – Controls Mac's content filters and other parental settings
- **Time Machine** – Controls the behavior of Mac's built-in, user-friendly backup and recovery system

By centrally managing these settings, you can significantly increase the security, stability, and efficiency of your Mac desktops, which improves reliability, productivity, and even compliance. For example, you can enforce backup policies so that Mac computers use Time Machine to perform regular content backups. You can also enforce login policies so that Mac computers connect to the proper Active Directory domains as well as key system preferences to enforce full-volume encryption and the use and operation of password-locked screen savers.

Even individual application settings can be controlled. In the Mac world, applications store their preferences in easily-accessible locations. Application vendors provide *preference manifest files,* which "explain" to Group Policy which settings the application should expose to management. These manifest files can actually be embedded directly within the application, making them easily accessible. These files extend your ability to control application settings through Group Policy.

In fact, there's almost nothing on a Mac that you *can't* control through Group Policy. Authentication Services gives you literally thousands of options for improving security, efficiency, stability, and compliance—all from a single, central point of control.

Summary: Windows and Mac - A Happy Co-existence

There's no reason to fear future Mac ownership; there are significant business benefits in diversifying your computer base, selecting the "right tool for the right job" and giving your users the computers that they need to be comfortable and productive. None of those advantages need to be overshadowed by increased management issues: with Quest Authentication Services, your Mac computers can enjoy the same authentication, single sign-on, and policy-based management capabilities as your Windows computers. Quest Authentication Services enables this through your *existing* AD infrastructure investment, not a separate, parallel system. This enables so your administrators to continue working the way they do now, without additional expensive training and an intrusive implementation.

Let your business be flexible and capable with a range of operating systems, and let Quest Authentication Services make it as easy to manage as a homogeneous environment.

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 a recipient of the Microsoft Most Valuable Professional Award 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 Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit **www.quest.com** for more information.

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)
If you are located outside North America, you can find your local office information on our Web site.

E-MAIL **sales@quest.com**

MAIL Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

WEB SITE **www.quest.com**

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 **https://support.quest.com**.

SupportLink gives users of Quest Software products the ability to:

- Search Quest's online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.

QUEST SOFTWARE
Smart Systems Management

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.

WPW-ManagingMacs-US-AG-20091203