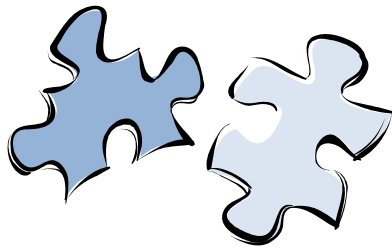




## The Value of Desktop Authority on the Well-Managed Network

A ScriptLogic Product Positioning Paper



### Desktop Authority - The Missing Piece

You've invested in a desktop management platform, but your desktop ownership costs could still be much lower...

# Desktop Authority and the Well-Managed Network

---

## Executive Summary

Organizations of all sizes need a comprehensive solution to cope with the many challenges present in managing Windows desktops. Desktop configuration, software deployment, remote management, power management, patch application and asset management are all essential building blocks to maintaining a secure and consistent desktop. Many organizations have chosen vendors such as Altiris, LANDesk, or Microsoft's Systems Management Server (SMS) or its successor, System Center Configuration Manager (SCCM) as their underlying desktop management platform. These solutions give the administrator of the well-managed network centralized control over software management, inventory and other key features.

In this paper, we will present the benefits of using Desktop Authority, a leading desktop management tool for Windows based networks, as an incremental solution to complement and expand the functionality provided by these platforms. In particular, we will focus on how Desktop Authority delivers a secure and consistent desktop, eliminates logon scripts, protects against data theft, enforces power management, removes spyware, and much more. If you have already chosen SMS/SCCM or any other enterprise solution as your established desktop management tool, this paper will demonstrate why Desktop Authority is an essential addition to your network management infrastructure.

## Desktop Authority – Essential Features for the Well Managed Network

Desktop Authority was originally developed as a graphical alternative to hand-coded logon scripts and managing the basic day-to-day challenges of a desktop administrator. From that initial concept, the product grew into a far-reaching desktop lifecycle management solution that uses a powerful graphical interface to tackle issues such as desktop configuration, power management, remote assistance, and provides other valuable benefits to the desktop administrator.

In particular, Desktop Authority gives the IT professional centralized, granular, and integrated control of the desktop in the following areas:

1. Delivery of a consistent and secured user workspace
2. Power management and inactivity monitoring
3. Logon scripts eliminated and Group Policy simplified
4. Prevent data theft and audit use of removable storage devices
5. Excellent remote management capabilities
6. Protection against spyware and adware infections

## 1. Delivery of a consistent and secured user workspace

Employees need the ability to access important applications and resources the first time, every time. Additionally, they need a task-oriented workspace optimized for their requirements, no matter which workstation they are using.

Desktop Authority's comprehensive configuration options combined with its patented Validation Logic technology provides unlimited flexibility in providing a workspace optimized for each user, group, location and environment.

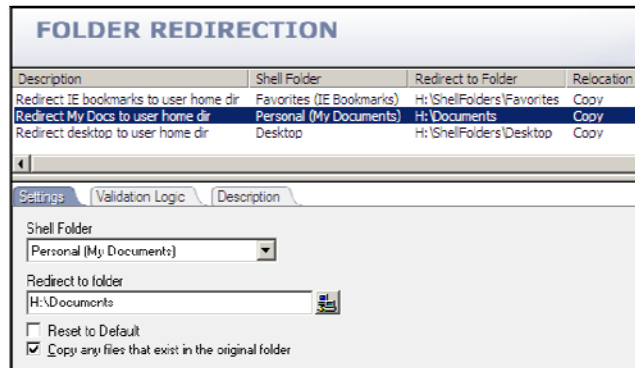


Figure 1: Simplify and customize the applications available from the start menu and the desktop.

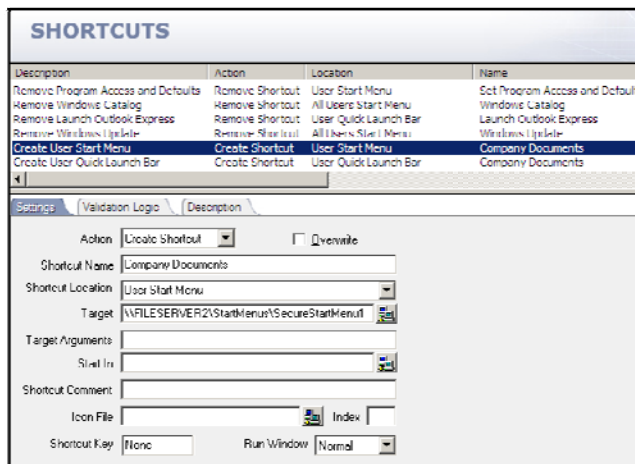


Figure 2: Provide predefined sets of applications and data by redirecting common folders, such as the Common Programs group.

## 2. Power management and inactivity monitoring

The U.S. Environmental Protection Agency estimates that 58% of the business day, computers are sitting idle and only 36% of all computers are shut off after business hours. Desktop Authority provides administrators the ability to manage power schemes in order to achieve maximum energy savings during work hours. From a single management console, configuring and reporting on power management settings is simplified. Granular configuration on all aspects of Windows power options such as power schemes, advanced power button settings, and hibernation settings is achieved through

the use of Validation Logic. This patented technology allows administrators to determine how each desktop will be configured and provides a means to granularly select which users and computers receive each setting, resulting in raised productivity and lowered energy usage.

In a recent customer testimonial from Bonneville Joint School District No. 93, the use of the power management scheme ALONE in Desktop Authority saved them **\$36,000 a year!**

Report Parameters: Computer Name: All, Computer OU: All, Scanned Since: 12/20/2006 12:00:00 AM, % of Desktops with LCD Monitors: 100, % Daily Inactivity During Work Day: 50, Energy Cost Per kWh (\$): 0.0067, Hours Per Standard Work Day: 8, Days Per Standard Work Week: 5, Min Inactivity Before Monitor Shut Off: 30, Min Inactivity Before HII Shut Off: Never, Min Inactivity Before Stand-By: 60	
<b>Summary of Inputs</b>	
Number of Desktops with CRT Monitors	0
Number of Desktops with LCD Monitors	99
Number of Laptops	28
Energy Cost per kWh *	\$0.0867
Hours in a standard workday	8
Days in a standard workweek	5
% of inactivity during the workday **	58.0%
Minutes of Inactivity before monitor shut-off	30
Minutes of Inactivity before hard drive shut-off	Never
Minutes of Inactivity before system stand-by	60
<b>Current Energy Costs</b>	
Avg Energy Cost per Work Day with No Power Management	\$23.72
Avg Energy Cost per Non-Work Day with No Power Management	\$21.96
<b>Power Managed Energy Costs</b>	
Avg Energy Cost per Work Day with Power Management	\$9.58
Avg Energy Cost per Non-Work Day with Power Management	\$0.78
<b>Power Savings</b>	
Saved Energy Cost per Work Day with Power Management	\$14.15
Saved Energy Cost per Non-Work Day with Power Management	\$21.18
<b>Saved Energy Cost Per Year with Power Management</b>	<b>\$5,880.99</b>

Figure 3: Based on defined settings and the actual hardware in your organization, Desktop Authority can provide a customizable power savings report to depict an estimate of “energy saved” in your organization. This flexible reporting also simplifies the ability to perform ‘what-if’ scenarios and illustrate how setting and hardware changes could potentially affect your power savings.

### 3. Logon Scripts Eliminated and Group Policy Simplified

Many configuration tasks, such as mapping drives and configuring printers, traditionally rely on logon scripts. Another approach to desktop configuration is to use Group Policies. Scripts can be slow, difficult to maintain and require costly expertise, and achieving the same result with Group Policies can become complex, particularly if you’re trying to manage something that doesn’t fit in the Active Directory structure.

Desktop Authority eliminates the need for hand-coded logon scripts, decreases the complexity that often comes with using large numbers of Group Policies, and can dramatically reduce logon times. In recent customer situations we have seen examples where Desktop Authority has reduced logon times from **2 minutes to 25 seconds!**

With Desktop Authority’s intuitive graphical interface, deployment of settings that would normally require extensive scripting or the use of many Group Policies can be achieved with just a few mouse clicks.

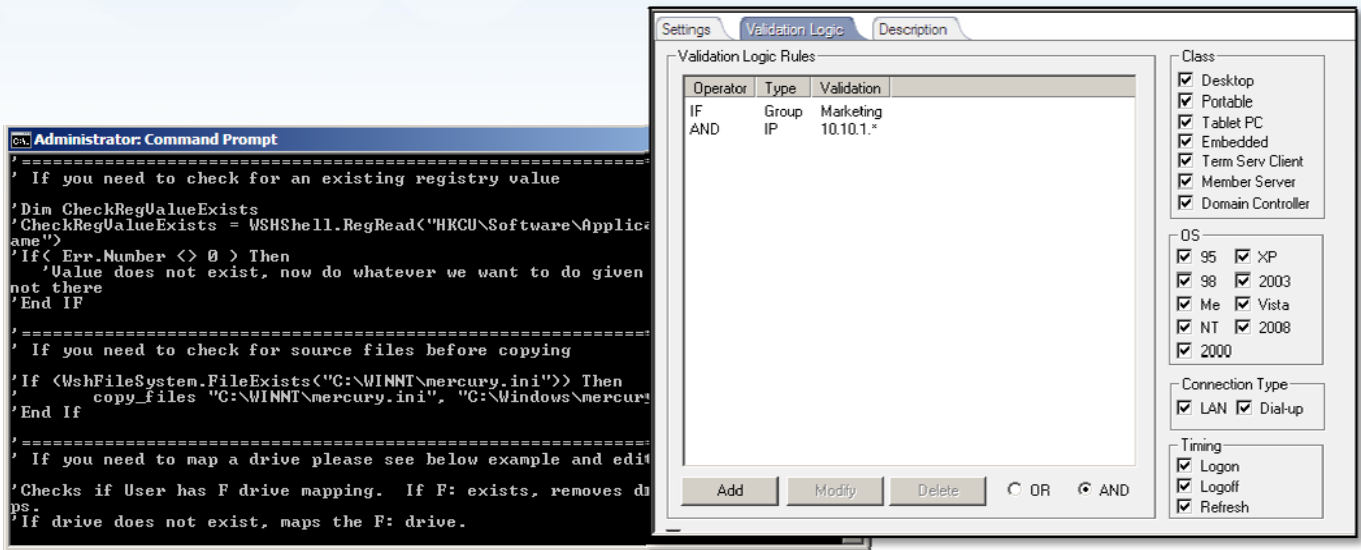


Figure 4: Replace complex, time-consuming scripting with simple, easy to use graphical configuration.

#### 4. Data Theft Prevention

The use of removable media devices has become one of the most widely used methods of storing data, but because of both internal and external regulations, new safeguards need to be implemented to prevent the removal or copying of sensitive data on these devices. Copying data, introducing viruses, and installing illegal software on the company network are all issues that must be addressed, and Desktop Authority USB & Port Security, shown in Figure 5, tackles these issues head-on.

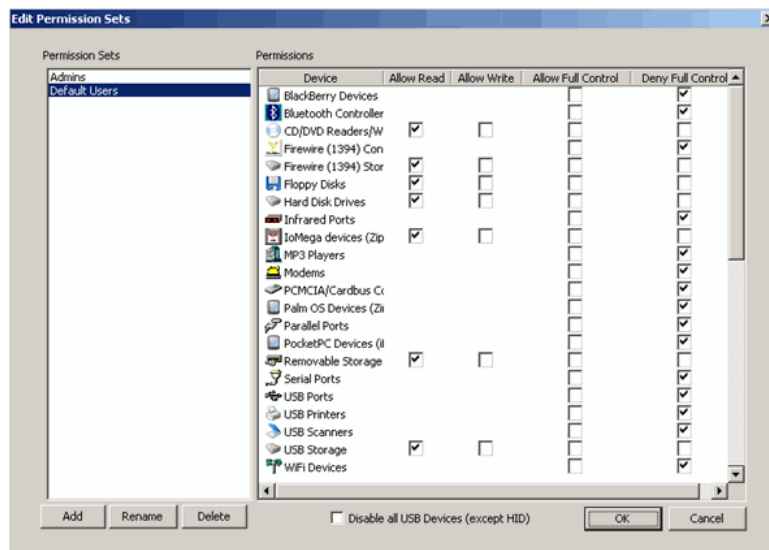


Figure 5: Desktop Authority provides policy-based lockdown of USB, storage and communication devices with multiple levels of security to allow complete access or denial to certain device types

With granular control over each device type, organizations can limit usability of certain devices to “read” but not “write” or allow users to “read” CDs or DVDs, but not “burn” them. Granular control over who has permissions to use certain devices either based on their AD group/site, IP subnets, computer class, type of device, or any other established factor is easily achieved.

## 5. Advanced Remote Management: More Than Remote Control

Desktop Authority’s remote management goes far beyond the traditional remote control functionality available through other vendors and extends that reach by offering true remote management on nearly every aspect of the client operating system. Using a dashboard view, administrators can troubleshoot desktops without interrupting user productivity. Whether it’s adding files to the computer, troubleshooting runaway processes or evaluating performance statistics, administrators have complete authority over the remote desktop. Furthermore, multiple levels of administrator privilege are provided so only approved administrators can carry out privileged operations like shadowing a desktop, or deleting files, and the user’s permission is usually required before the support staff can actually see the contents of their screen. A chat function, performance statistics, diagnostic tools, remote command prompt and registry access are also provided to simplify the troubleshooting process.

In one customer case study performed by Forrester, without the use of Desktop Authority’s functionality the organization would have had to hire and incur the **costs for three to four more technicians**.

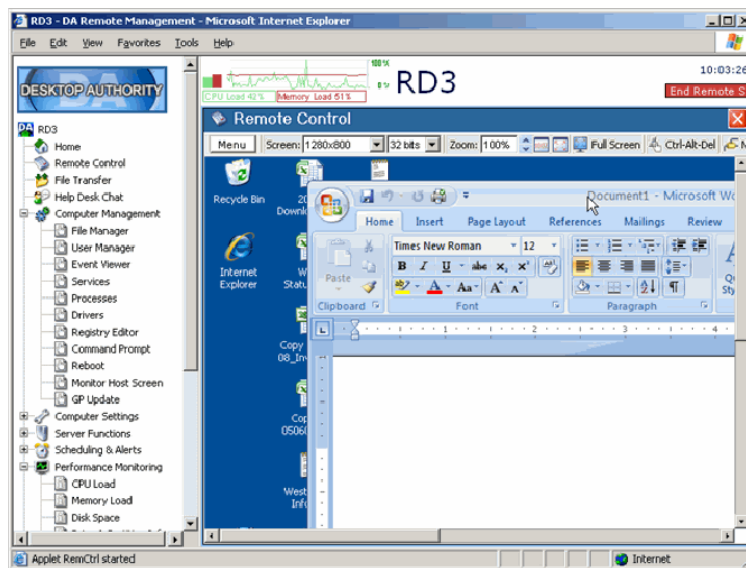


Figure 6: Desktop Authority’s remote assistance capabilities give administrators complete authority over the remote desktop, including background access to the file system, services, programs and system status without interrupting the end user.

## 6. Spyware Detection and Removal

With 20-40% of all helpdesk calls being contributed to spyware and adware infections, it is apparent that the task of detecting and removing malware from the desktop requires more than reliance on perimeter network security. And, with the majority of anti-spyware solutions targeting the individual user only, the need for a centralized detection and reporting mechanism is vital to ensure continued security in the enterprise.

Desktop Authority Spyware Detection and Removal option gives administrators the ability to centrally secure and protect desktops across the enterprise against spyware. This protection, coupled with centralized control and reporting enables administrators to take full advantage of a threat detection community, secure all desktops against a wide range of attacks, and report on the presence of network intrusions.



Threat Name	Category
Trojan-Downloader.Zlob.Media-Codec	Trojan Downloader
Trojan.FakeAlert	Trojan
Adware.Mostofate (v)	Adware (General)
Virtumonde	Adware (General)
Antivirus.XP.2008 (Winifixer)	Rogue Security Program
Adware.NetAdware.Gen	Toolbar
FakeAlert.PCHealthCenter	Trojan
Trojan.NewMediaCodec	Trojan Downloader
Trojan.Win32.Monder.gen	Trojan
MS Antivirus(MSA)	Rogue Security Program

Live Stats Provided by CounterSpy and VIPRE

Figure 7: “Top 10” Spyware threats discovered by Threatnet, the basis for Desktop Authority’s Anti-Spyware engine.

## Desktop Authority Product Family

The Desktop Authority family of products also offers additional solutions outside the core components of traditional desktop management. This add-on functionality expands the already robust Desktop Authority offering, and augments the well-managed network in areas that affect desktop administrators every day.

## Seamless Integration for MSI Deployment

Software deployment through System Center Configuration Manager works best when using MSI packages. However, MSI packages often require customization for successful installation, and legacy setup packages need to be repackaged as MSI files. ScriptLogic offers MSI Studio for Configuration

Manager which has an easy to use, administrator focused interface for repackaging legacy installs, creating MSI transforms, and creating patches for MSI files.

MSI Studio for Configuration Manager, shown in Figure 8, integrates seamlessly with Microsoft System Center Configuration Manager 2007. When you have completed and tested an MSI package, MSI Studio can pass that package to Configuration Manager and automatically add package details to the management database.

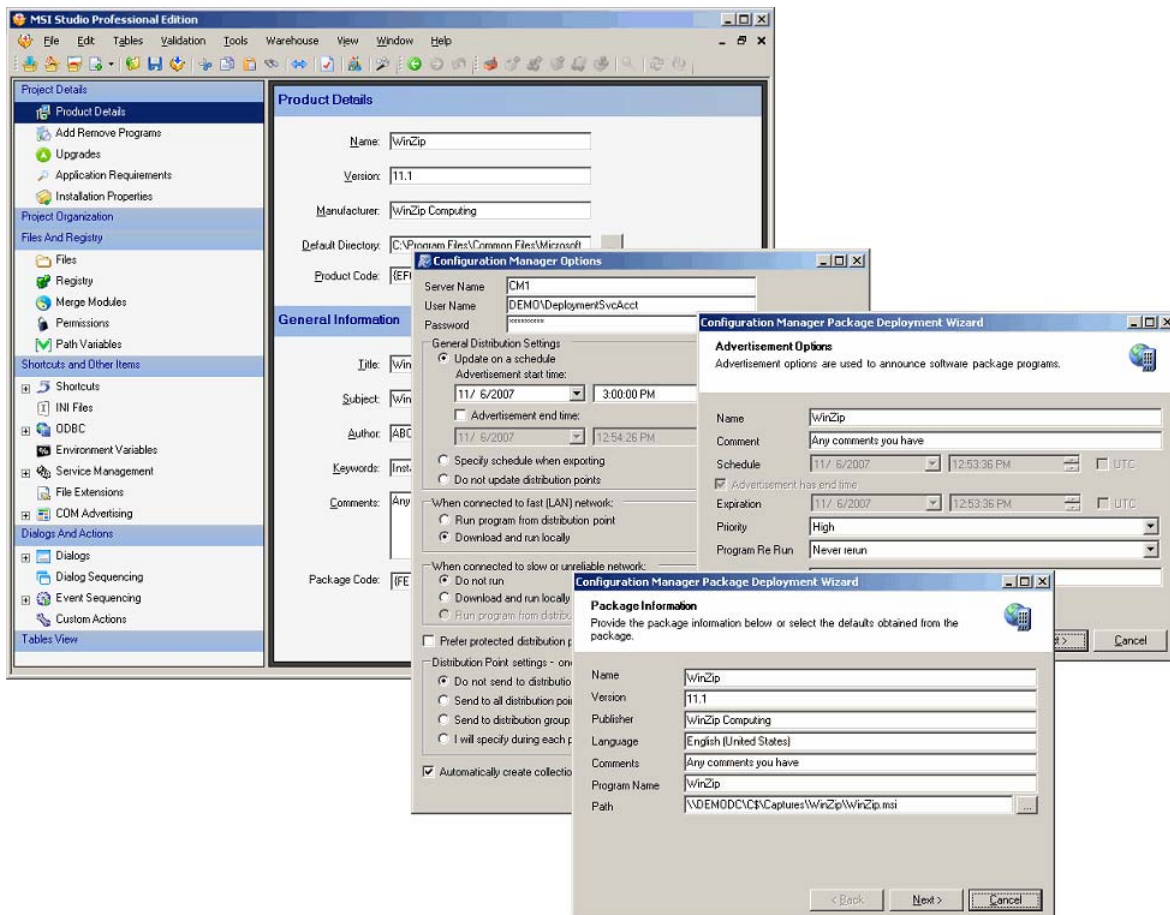


Figure 8: MSI Studio for SCCM seamlessly integrates the publishing of packaged application installers.

Other key benefits of MSI Studio include:

- **Zero-Touch Testing** - allows you to easily create a special MSI package which simulates the effect of the application installer on the target computer, but without actually making any changes. The administrator can identify which files and registry keys which will be overwritten and changed without doing any damage.
- **Conflict Resolution** - adds a repository for storing MSI packages, which offers easy reporting on potential package conflicts.

## Password Management: The Right Way!

According to numerous industry experts, nearly 45% of all helpdesk calls are password related. Yet more and more stringent security policies are being implemented at every organization, on every department level which demand stricter password controls. With Desktop Authority Password Self-Service you can help the end users become more productive, decrease your end-user support cost, and increase security. Leveraging your existing Active Directory infrastructure, end-users can reset their passwords and unlock accounts through a web interface without having to contact the help desk.

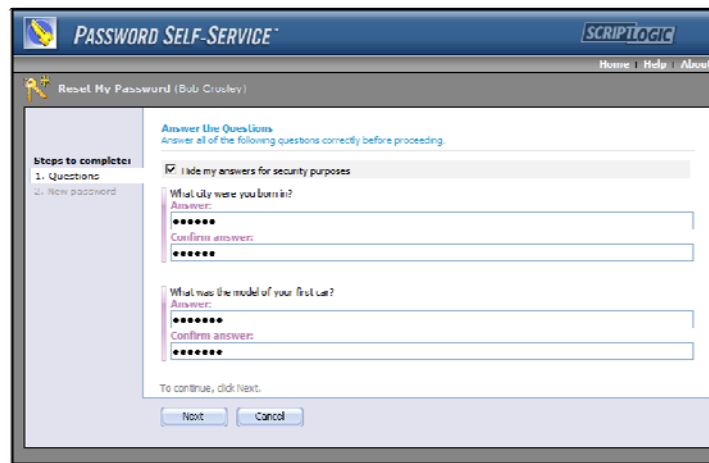


Figure 9: Desktop Authority Password Self-Service provides personal Q&A profiles for each user containing questions with very unique answers that are easy for users to remember, but hard for others to guess.

Implementing a password management solution allows organizations to:

- ✓ Increase security by eliminating help desk errors
- ✓ Reduce the need for users to write down their password
- ✓ Enforce administrator defined standards

## Conclusion

ScriptLogic's Desktop Authority is an award-winning solution that has been helping desktop administrators manage and control the desktop lifecycle since 1999. It can reduce the total cost of ownership for desktops by reducing help desk calls, managing power more efficiently, restricting the use of removable storage, providing advanced remote assistance, and keeping your desktops patched and secured as well as replacing hand-coded, cumbersome logon scripts.

Microsoft's SMS/SCCM, along with a number of other solutions, addresses core Windows desktop administration concerns. However there are numerous other facets of day-to-day desktop management that are not covered and result in considerable cost overheads for the IT department and the wider workforce. Centralizing and automating routine desktop maintenance tasks delivers further cost savings, greater efficiencies and tighter security, and this additional functionality can be found in ScriptLogic's Desktop Authority product family.

## About ScriptLogic

[ScriptLogic Corporation](#) is a leading global provider of systems lifecycle management solutions for Microsoft Windows-based networks. ScriptLogic's award-winning suite of Desktop management software, Server management software, Active Directory management software, and Help Desk software products help empower network administrators to proactively save time, increase security, and maintain regulatory compliance. More than 23,200 customers use ScriptLogic solutions to manage approximately 5.7 million desktops and 138,000 servers. ScriptLogic solutions benefit any size network in any industry. ScriptLogic, headquartered in Boca Raton, Florida, is a wholly owned subsidiary of Quest Software, Inc. (Nasdaq: QSFT). Reach ScriptLogic at (561) 886-2400 or on the Web at <http://www.scriptlogic.com>.

© 2008 ScriptLogic Corporation. All Rights Reserved.