



DESKTOP AUTHORITY® AND AD GROUP POLICY OBJECTS

A ScriptLogic
Product
Positioning
Whitepaper

NICK CAVALANCIA

INTRODUCTION

As more and more organizations adopt Windows 2003 and Active Directory for their networks, IT departments looking for a desktop management solution begin to evaluate both the capabilities inherent with Windows, as well as third-party solutions to determine which will best meet their needs. Desktop Authority becomes a leading contender because of its comprehensive desktop configuration abilities coupled with its powerful Validation Logic. But organizations cannot ignore the functionality built into Group Policies either. So the question is inevitably raised, “Can’t I accomplish everything I need with Active Directory and Group Policy Objects?”

The answer is simple – alone, Group Policies are not enough. Both Desktop Authority and Group Policy Objects (GPOs) are great management tools – each product provides an effective means of reducing the amount of time (and money) that is required to effectively manage networked PCs and thin clients. In fact, the most successful Active Directory deployments are environments that use both Desktop Authority and Group Policies.

Group Policy Objects, while a robust form of management, are not necessarily the best approach to accomplishing all types of administration tasks. Think about the name – a ‘policy’ is something you establish and infrequently change. Event Log settings, for example, are where GPOs are well suited. The day-to-day changes users require, like an additional drive mapping or a new shortcut on their desktop is not something easily accomplished with Group Policies. This is where the intuitive design of Desktop Authority becomes the perfect complement to Active Directory and GPOs.

Active Directory is a server-side component, and so are Group Policy Objects. All the classifications of which settings apply to you and the workstation you log onto are stored within AD well before you ever log on. This approach has numerous limitations, and unlike Desktop Authority, does not offer “real time” dynamic change – like support for when a user logs on from a variety of workstation operating systems,

or applying a configuration setting one way if the user logs on from a desktop, but a different way should the user log on from a portable computer.

To use an analogy, let’s say you were developing a web site that would run on a Microsoft IIS server. To provide dynamic page content, would you choose Active Server Pages (ASP) or JavaScript (JS)? If you chose only one, you’d be selling your website short of its potential – there is a benefit and a need for both technologies. ASP code is processed by the server, before the page is displayed to the browser, and JavaScript is processed by the browser, at runtime, on the client. Today, you’d be hard-pressed to find a quality website that didn’t employ both ASP and JS.

GPOs and Desktop Authority have that same symbiotic relationship as ASP and JavaScript. The settings stored in server/domain level. Desktop Authority dynamically bases its decision to apply configuration settings at the client, during the logon process. The end result is complete coverage of client configuration – the long-term settings are assigned by GPOs and the everyday changes are made by Desktop Authority.

“The most successful Active Directory deployments are environments that use both Desktop Authority and Group Policies.”

In the following sections of this whitepaper, I will compare Desktop Authority and GPOs as management tools in four important areas – platforms supported, management functionality, management granularity and overall ease of use. These comparisons apply equally as well to ScriptLogic Enterprise as they do to Desktop Authority. Remember, the purpose of this document is not to make you choose one tool, but rather to identify the benefits of using both Desktop Authority and GPOs in concert.

WHICH OPERATING SYSTEM DO YOU HAVE?

The most obvious difference between the two tools is the Operating System (OS) platforms that can be managed by each. Group Policy Objects (GPOs) can manage only Windows 2000 and Windows XP-based machines. If you're privileged enough to have a pure Windows 2000 environment or newer, you may think this isn't an issue for you. However, GPOs can only differentiate between XP and 2000 if you utilize WMI Filters in a Windows 2003 AD, or put each set of workstations in a separate Organizational Unit (OU) and make different GPOs for each OU in a Windows 2000 AD. This means there is no true central management for both operating systems.

While GPOs can only manage Windows 2000 and XP clients, Desktop Authority can manage and differentiate between clients running 95, 98, Me, NT, 2000 and XP, as shown in Table 1. Remember that Desktop Authority makes its determination at the client, at runtime. Because of this, Desktop

Authority can also tell if your client is a Desktop, Portable, Tablet PC, Embedded Windows, Terminal Server session, Member Server or a Domain Controller. Additionally, Desktop Authority can detect whether you're logging on from a LAN-based computer or connecting over a dial-up connection via DUNS. (See Figure 1).

Platform	GPO	Desktop Authority
Windows XP Pro	✓	✓
Windows 2000 Pro	✓	✓
Windows NT 4.0 Wks		✓
Windows Me		✓
Windows 98		✓
Windows 95		✓

Table 1: Operating Systems supported

Desktop Authority clearly provides better dynamic coverage of not just mixed client networks, but even networks with Windows 2000 and XP. Next, let's look at what each tool can do to the clients it manages.

WHAT DO YOU WANT TO MANAGE TODAY?

One of the reasons Microsoft made such a huge deal about GPOs when Windows 2000 was released is because it is a great way to manage desktops in a native environment (if you have a mixed environment, you already know this is a moot point for you). Let's suppose you are running a native environment, with only Windows 2000 or XP clients – Is Desktop Authority still needed? Let's look at the management abilities of each product to answer this question.

GPOs, without GPO extensions, supplemental batch files, resource kit utilities, VB/WSH or KiX scripts called on to perform tasks, by default have three components: Software Installation and Maintenance, Security Settings, and Administrative Templates. The software installs are accomplished by using Microsoft Installer files (MSIs) and can be **published** or **assigned** to a Windows client. Publishing an application will list it in the Add/Remove Programs Control Panel applet. Assigning an application will place icons on the Start Menu and create file extension associations as well as publish it. When assigned, you can double-click the application icon in the start menu or a document with an associated extension and the application will be installed on demand. The security settings establish

settings such as Password Policies, Event Logs and Local Policies (e.g.: user rights and audit settings). However, most of the functionality gained from GPOs comes in the form of Administrative Templates.

Administrative Templates manage numerous aspects of the workstation through registry changes: desktop settings, folder redirection, application settings for Internet Explorer (IE), NetMeeting, Windows Messenger, Windows Media Player, Office, with each of these settings defined in an Administrative Template (a .ADM file) to be pushed out via Group Policies. Because software vendors and administrators alike can generate their own templates to push out desired settings, this aspect of GPOs is somewhat limitless, with new templates being published often.

With its ability to import Group Policy template settings, Desktop Authority not only levels the playing field with regard to the functionality gained with Administrative Templates, but actually surpasses Group Policy functionality by its use of patented Validation Logic technology to selectively implement the template settings (see the next section for more information on Validation Logic).

Table 2 lists the management abilities of both Desktop Authority and GPOs. Keep in mind that the capabilities of GPOs are limited to Windows 2000 and XP clients, while Desktop Authority's capabilities (with the exception of Administrative Template-based settings) extend to all clients from 95 to XP.

Native management feature	GPO	Desktop Authority
Logon, Logoff & shut down scripting	✓	✓
Software deployment	✓	✓
Permissions for registry and file system	✓	✓
Windows Firewall (XP) settings	✓	✓
All settings available within Administrative Templates	✓	✓
Password and account lockout policy	✓	
Local policies (auditing, user rights)	✓	
Event log settings	✓	
Restricted groups	✓	
Services management	✓	
Inactivity Timer (to logoff, shutdown or restart)		✓
Patch Management		✓
Anti-Spyware		✓
File Operations (copy, move, delete)		✓
Drive mappings		✓
Search paths		✓
Add/remove printers (Network & IP)		✓
Time synchronization		✓
Outlook/Exchange mail profile creation		✓
Add/remove registry settings		✓
Manipulate INI files		✓
Environment variable management		✓
Shortcut management		✓
Microsoft Office open/save paths		✓
Execution of applications		✓
Displays messages during logon		✓

Table 2: Features Comparison

In Table 2 you may have noticed that some features are not available in Desktop Authority. I would like to point out two issues with those specific features. First, they only apply to Windows 2000 and XP clients. Second, they are related to changes that usually need only to be made once and not changed on a daily basis. So Group Policies play a role with

long-term policies you may put in place for your workstations, whereas Desktop Authority plays a role in the day-to-day and long-term configuration of those same desktops. For example, GPOs would be best suited for setting the size of your event logs, whereas Desktop Authority would be your best solution to establish drive mappings and add printers.

HOW LOW CAN YOU GO?

It's great to have a robust management tool, but if that tool doesn't allow you to establish the proper criteria before applying settings, you're left with the daunting task of manually applying selective changes to a multitude of desktops on your network – so let's talk about management granularity.

GPOs can be applied at the Domain, Organizational Unit, and Site levels within Active Directory. Further granularity is available by changing the security settings to have a GPO only apply to a group or user within the domain, OU or site. Windows 2003-based AD environments can take advantage of WMI Filtering. WMI Filtering is limited to client-side information and involves filter generation similar to scripting.

In contrast, at the heart of each configuration setting within Desktop Authority lies "Validation Logic" – a unique technology with 35 different GUI-based validation criteria

that allows you to be far more granular when assigning or applying a configuration setting, shown in Figure 1.

In addition to the Validation Logic Classes, Operating Systems and Connection Types, you can enlarge the selection criteria through the use of wildcards {?,*} for the Type's Value to determine the applicable clients. In the example below, an entire TCP/IP subnet could be specified as the condition which must be met prior to deploying a printer to a collection of desktops.

Desktop Authority also allows you to enter in multiple values utilizing Boolean logic making Validation Logic exponentially more granular. Because Validation Logic can be applied to each element AND at the configuration profile level, you can establish a hierarchy that scales to multi-location enterprises, yet can be tailored to an individual user's requirements.

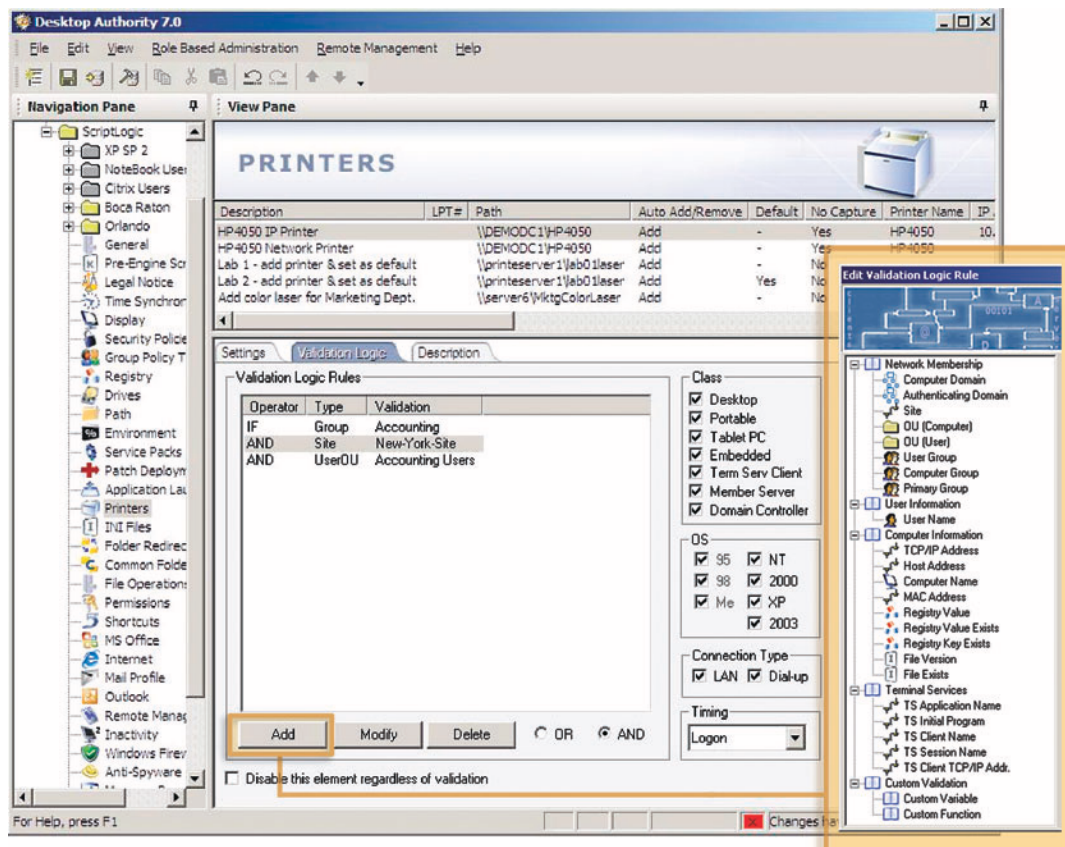


Figure 1: Desktop Authority's intuitive user interface with extensive configurations and Validation Logic settings.

Table 3 compares the native levels of granularity found in both Desktop Authority's Validation Logic and GPOs. Note, this table does not take into account the additional criteria possible if an administrator was to script custom WMI Filtering queries.

Granularity Elements	GPO	DA Validation Logic
Class of Machine (Desktop, Portable, DC, etc)		✓
Operating System (95, 98, ME, NT, 2000, XP, 2003)		✓
Connection Type (LAN, Dialup)		✓
Computer Domain		✓
Authenticating Domain		✓
Active Directory Site	✓	✓
OU (Computer)	✓	✓
OU (User)	✓	✓
User Group	✓	✓
Computer Group	✓	✓
Primary Group		✓
Username	✓	✓
TCP/IP Address (including subnets)		✓
Host Address		✓
Computer Name		✓
MAC Address		✓
Registry Value		✓
Registry Value Exists		✓
Registry Key Exists		✓
File Version		✓
File Exists		✓
Terminal Services Application Name		✓
Terminal Services Initial Program		✓
Terminal Services Client Name		✓
Terminal Services Session Name		✓
Terminal Services Client TCP/IP Address		✓
Custom Validation (using Kix scripting)		✓
Support for Multiple Values		✓
Support for Boolean Logic (NOT, AND, OR)		✓

Table 3: Selection criteria used to implement configuration settings.

Even with WMI Filtering, Group Policies can't come close to providing the same level of granularity that Desktop Authority's Validation Logic does – because, as previously mentioned, either the GPO configuration is determined by Active Directory, prior to the logon process or cannot be

attained through a WMI Filter. With none of this vital information readily available to GPOs by design, you lose the granularity Desktop Authority takes advantage of by determining the client validation at logon.

JUST HOW EASY SHOULD IT BE?

Despite the feature sets, the interface and overall ease of use can make or break a product. Windows 2000 domains use the Group Policy Editor Microsoft Management Console (MMC) interface, while Windows 2003 domains use the new Group Policy Management Console to navigate to and edit GPOs. Desktop Authority also has its own intuitive interface. While each interface has the same underlying design goal – to be intuitive and easy to use, the difference comes when you want to make changes to users that have different needs. GPO editing is a decentralized process, since two separate settings in AD would require two GPOs and, therefore, two separate changes (one in each policy). Desktop Authority

enjoys a single, centralized interface where all of the settings are found. Two separate settings would simply be listed as two lines in within the same interface. Should you desire a separation of configuration settings based on any of the Validation Logic parameters, Desktop Authority does support multiple configuration profiles. Additionally, Desktop Authority features built-in reporting on both the configurations created within Desktop Authority, as well as additional reporting on hardware/software inventory, user activity, anti-spyware deployment and patch distribution using pre-defined and custom reports.

SUMMARY

Both Desktop Authority and Group Policy Objects are powerful management tools – each product provides an effective means of reducing the burden that is typically associated with maintenance of PCs and thin clients in a networked environment.

In a mixed platform network, GPOs cannot be effectively used as a single management tool. In a pure 2000/XP

environment they will provide an effective, yet limited, means of desktop management.

With its complete support for all Win32 desktop platforms, richer management feature set, deeper level of management granularity, simplified configuration approach, and administrative reporting, Desktop Authority is a necessary complement to the limited desktop management capabilities offered by GPOs.

For more information, contact ScriptLogic at: www.scriptlogic.com | 1.800.424.9411 | 1.561.886.2400