



Desktop Authority and Group Policy Preferences

A ScriptLogic Product Positioning Paper

Desktop Authority and Group Policy Preferences

Introduction

Group Policy Preferences

In Windows Server 2008 and Windows Vista Service Pack 1, Microsoft introduced a Group Policy-based technology called Group Policy Preferences (GPP) derived from Policy Maker, a product acquired with DesktopStandard in 2006. This technology adds new Group Policy Extensions which provide extra Windows workspace configuration settings so Group Policy can be used, for example, to set up drive mappings and printer connections on a user's desktop. GPP also introduces "targeting", a technology which allows GPP settings to be selectively applied based on a range of user and computer properties.

Desktop Authority

ScriptLogic's Desktop Authority is an award-winning solution which centralizes and integrates a broad range of desktop management functions under one management console. Desktop Authority provides low-level desktop configuration, advanced remote assistance, security, desktop inventory and options for patch management, data theft prevention and spyware removal. Since 1999 ScriptLogic has been dramatically lowering the cost of desktop management for over 20,000 customers with more than 5 million Windows desktops managed.

This Paper

The addition of GPP in Windows demonstrates Microsoft's recognition of the cost savings and other benefits possible through centralized desktop configuration. This paper will explore the differences and overlap between ScriptLogic's Desktop Authority (DA) and Microsoft's GPP, and the benefits they offer. In particular it will look at the following areas:

1. Feature coverage
2. Granularity and flexibility
3. Ease of deployment
4. Troubleshooting

Feature Coverage

Desktop Authority started life as an alternative to the hand-coded logon scripts used for basic desktop configuration, and over the years it has grown its feature set to cover many other aspects of the desktop lifecycle, as is shown in the table below. The ability to manage the entire desktop lifecycle with one comprehensive solution is essential for Windows desktop administrators. Desktop Authority eases the administrator's burden and drives down the cost of Windows desktop ownership by enabling them to proactively control, inventory, secure, support, as well as configure desktops from a single location.

Despite this growth in features and coverage, Desktop Authority still retains a core focus on low-level, granular management of desktop settings. GPP also focuses on those core desktop configuration settings, with the aim of making Group Policy a more acceptable alternative to logon scripts. The following table highlights the breadth of coverage in the Desktop Authority family of solutions:

Product Feature	Desktop Authority	Group Policy including Preferences
Desktop Lifecycle Overview		
OS Provisioning	● †	
Application Packaging	● ‡	
Application Deployment	●	●
Desktop/User Workspace Configuration	●	●
Inactivity Monitoring and Actions	●	
Hardware and Software Inventory	●	
Software License Management	●	
Turnkey and Custom Reporting	●	
Advanced Remote Assistance	●	
Patch Management	●	
Data Theft Prevention (Port Security)	●	
Spyware Removal	●	

† Accomplished using Desktop Authority Image Center

‡ Accomplished using MSI Studio

Looking at the workspace configuration features in more detail, Desktop Authority also has more depth in some areas, especially in management of Microsoft Office settings and Outlook mail profiles. Unique management options offered through Desktop Authority include:

- Mandating standardized email signatures
- Enforcing auto archive settings
- Controlling whether to run a spell check on send
- Setting the default mail format

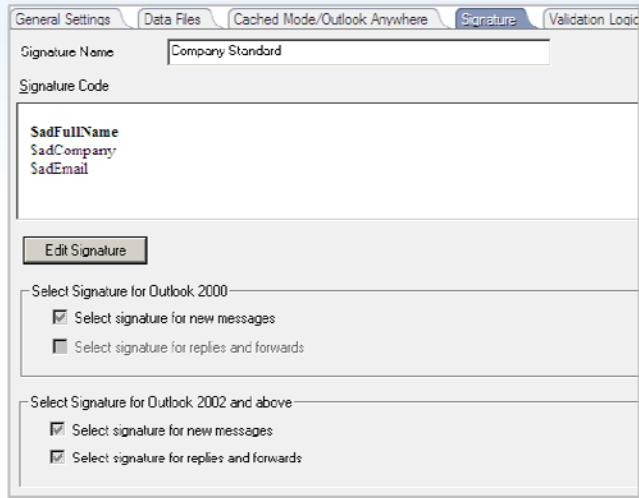


Figure 1: Desktop Authority's interface for creating standardized Outlook signatures, which can be populated with user and computer attributes, and varied by department, group, site or anything else defined in Validation Logic

With Desktop Authority, a user can log onto their computer for the first time and every setting (including Microsoft Office) is configured according to company standards, and reinforced every time the user logs on.

Granularity and Flexibility

It is imperative to have a desktop management and configuration solution that can adapt to your organization's ever-changing needs. GPP uses "Item-Level targeting" to apply desktop preferences based on criteria such as the version of Windows, the IP address of the desktop, and so on. Desktop Authority uses its patented Validation Logic to granularly filter configuration "elements" and achieve a similar effect. Depicted below is the terminology used to describe similar features in GPP and Desktop Authority:

Component	Desktop Authority	GPP
Individual configuration setting	Element	Item
Configuration Filtering	Validation Logic	Item-Level Targeting
Collection of configurations	Profile	Group Policy
Hierarchy of collections	Child Profiles	Group Policies linked to child OUs

Both Desktop Authority and GPP offer a wide range of user and computer criteria which determine when configuration settings are applied – known as targeting or Validation Logic. However, there are three key differences between Desktop Authority and GPP in how targeting or Validation Logic can be applied, and we will look at each in turn.

Validation Logic can be used Everywhere

Desktop Authority can apply Validation Logic on all areas of desktop management including security policies, application launching, software deployment, patch management and more. GPP offers targeting only on the items covered in the “Preferences” section of a Group Policy. To “target” the rest of the settings in Group Policy requires the use of WMI filters.

Some examples of the power of Validation Logic might help here:

- If you want to install a particular application for users in the “Sales Administrators” group, regardless of which OU they belong to
- If you want to restrict use of the Run command based (a Security Policy) for travelling users with laptops
- If you want to roll out only the most critical patch updates to users in remote offices across WAN connections
- If you want to lockout inactive desktops with different timeouts for computers in open areas and in secure offices, based on IP subnets

None of these examples can be easily achieved with GPP and Item-Level Targeting.

Figure 2 shows the various areas of desktop management handled by Desktop Authority. Each of these areas can be applied to desktops using Validation Logic.

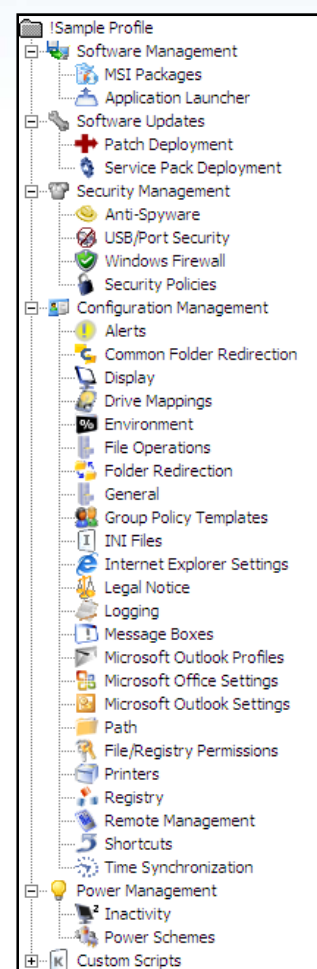


Figure 2: Validation Logic can be applied to every element type within the profile

Validation Logic can be applied on the Profile Level

Validation Logic can be applied at two levels in the profile: on an entire profile, or at the item (or “element”) level. Item-Level Targeting works only at the item level, not on the whole Group Policy or over a collection of items. For example, if your goal was to target all items in a Group Policy based on group membership, you would have to set that targeting on EVERY ITEM in the policy. In other words, if there were 100 items in a policy, you would have to configure targeting 100 times. On the other hand, Validation Logic allows you to set “targeting” just once at the profile level.

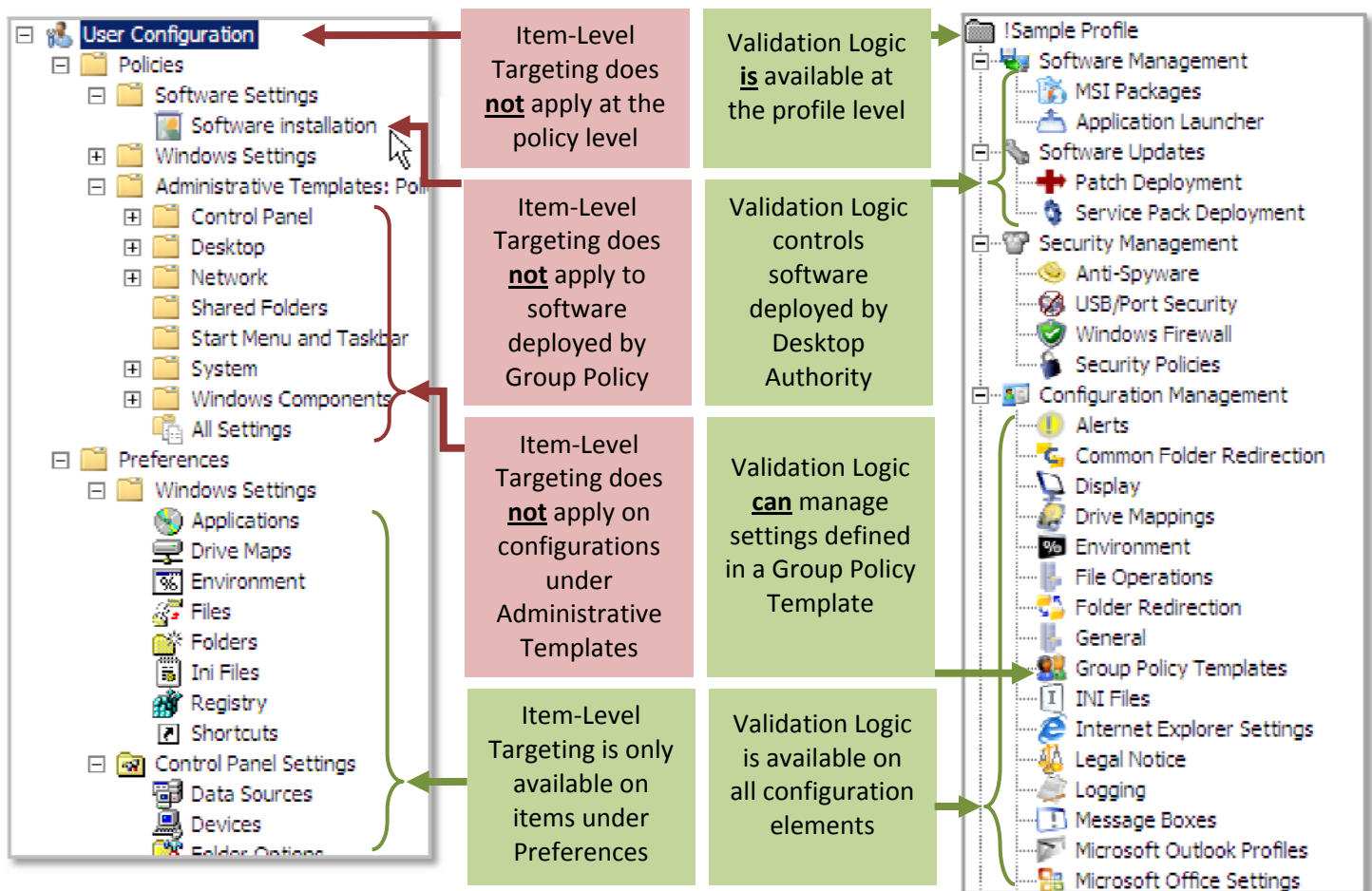


Figure 3: Desktop Authority's Validation Logic applies at both the element and profile levels, making targeting of the configuration easier and more controlled.

Validation Logic does not have to follow Active Directory's OU structure

GPP are a part of Group Policy, and Group Policies must be linked to an OU in Active Directory to take effect. Working independently of Active Directory with GPP requires a lot of editing of Item-Level Targeting on Group Policies which have been linked at the domain level, which is impractical.

Desktop Authority operates separately from the Active Directory OU structure. Profiles can be applied based on any criteria available in Validation Logic. Desktop Authority's configuration settings or "elements" are grouped into profiles, and profiles can be placed in a hierarchy with multiple child profiles, as shown in Figure 4. The benefit of this approach is the enormous flexibility Validation Logic provides by allowing you to build a hierarchy of configurations that map to:

- Your Organizational Unit in Active Directory, or
- Network Topology, or
- Functional Areas, or
- Geographical site locations, or
- Any combination of user and desktop properties.

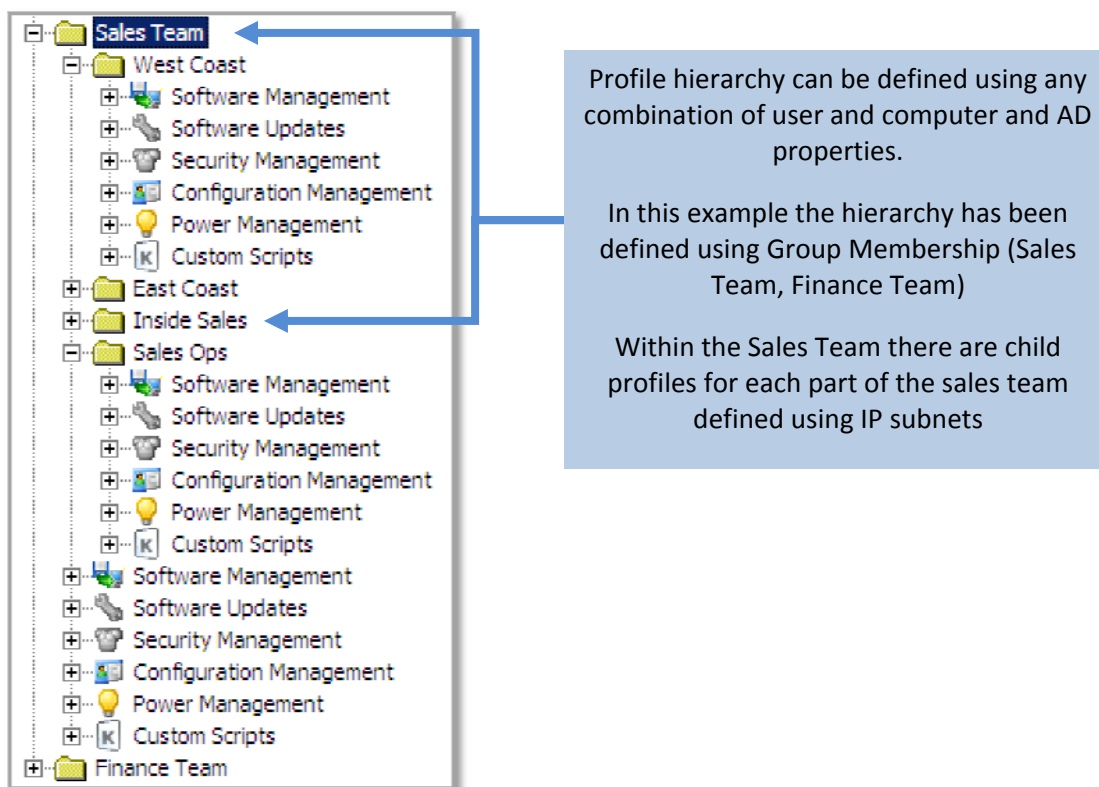


Figure 4: Using nested profiles, combined with Validation Logic, allows a simplified, flexible management hierarchy.

Ease of Deployment

Desktop Authority is installed centrally and is automatically deployed and configured when the user logs on, as shown in Figure 5. In fact, many users of Desktop Authority report that from initial download to actual machine management the time elapsed was less than one hour.

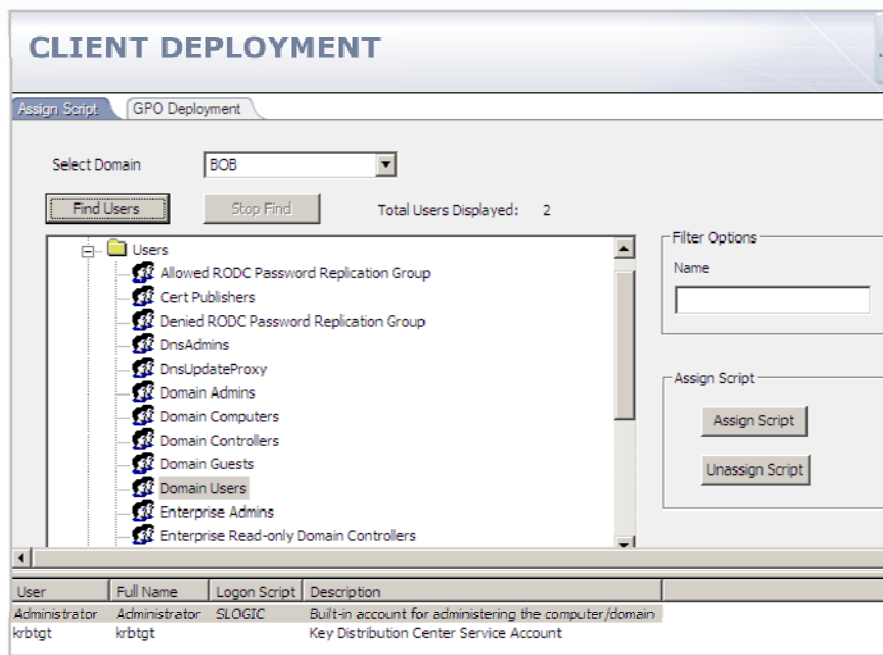


Figure 5: Desktop Authority's interface for selecting where the Desktop Authority client side components will be automatically installed

To manage computers with GPP you must install the Client Side Extension packs on the relevant desktops and servers. For different Windows versions the process is different – see the table below. To manage GPP you need at least one Vista Service Pack 1 or Windows Server 2008 computer available with the updated version of the Group Policy Editor.

Operating System	Desktop Authority	GPP
Installation of Client Side Components		
Windows 2000	Deployed from console	Not supported
Windows XP	Deployed from console	<ul style="list-style-type: none">- Requires SP2- CSE installer exe must be run from a logon script or SMS/SCCM- Also requires the XMLLite hotfix to be installed
Windows 2003	Deployed from console	<ul style="list-style-type: none">- Requires SP1- CSE installer exe must be run from a logon script or SMS/SCCM- Also requires the XMLLite hotfix to be installed
Windows Vista	Deployed from console	CSE installer can be run with Windows Update
Windows 2008	Deployed from console	Built-in as standard

Troubleshooting

Determining why an individual user or group of users did not receive a particular setting is one of the greatest challenges in configuring desktops. Why did that user not receive a patch? Why did the application not get installed? Desktop Authority can be centrally configured to record a trace log for selected (or all) users which let the administrator quickly identify the source of problems. This trace file, shown in Figure 6, is a commented HTML file that contains hot links to each section of the log so you can quickly jump to the profile element in question. Trace logs can be created by machine or user, and are automatically uploaded to a network share for centralized collection and analysis.



Figure 6: An example of Desktop Authority's trace log, with hyperlinks to every section of configuration settings

GPP offers reporting on policy items and item-level targeting, but there is no trace reporting for diagnosing why a setting was not applied, or whether an item succeeded or failed.

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.

With the introduction of GPP in Windows, Microsoft has validated the need for centralized desktop configuration as a way to drive down the cost of desktop ownership. The features in GPP overlap with Desktop Authority in two areas, namely logon script replacement and personalization of the user's workspace. However, there are some key differences in Desktop Authority, particularly that "targeting", or Validation Logic (as it is known in Desktop Authority) can be applied at a higher level and over all areas of desktop management, not just preferences.

For more information, please visit www.scriptlogic.com or contact your sales representative or preferred reseller for more information.

About ScriptLogic

[ScriptLogic Corporation](http://www.scriptlogic.com) 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.