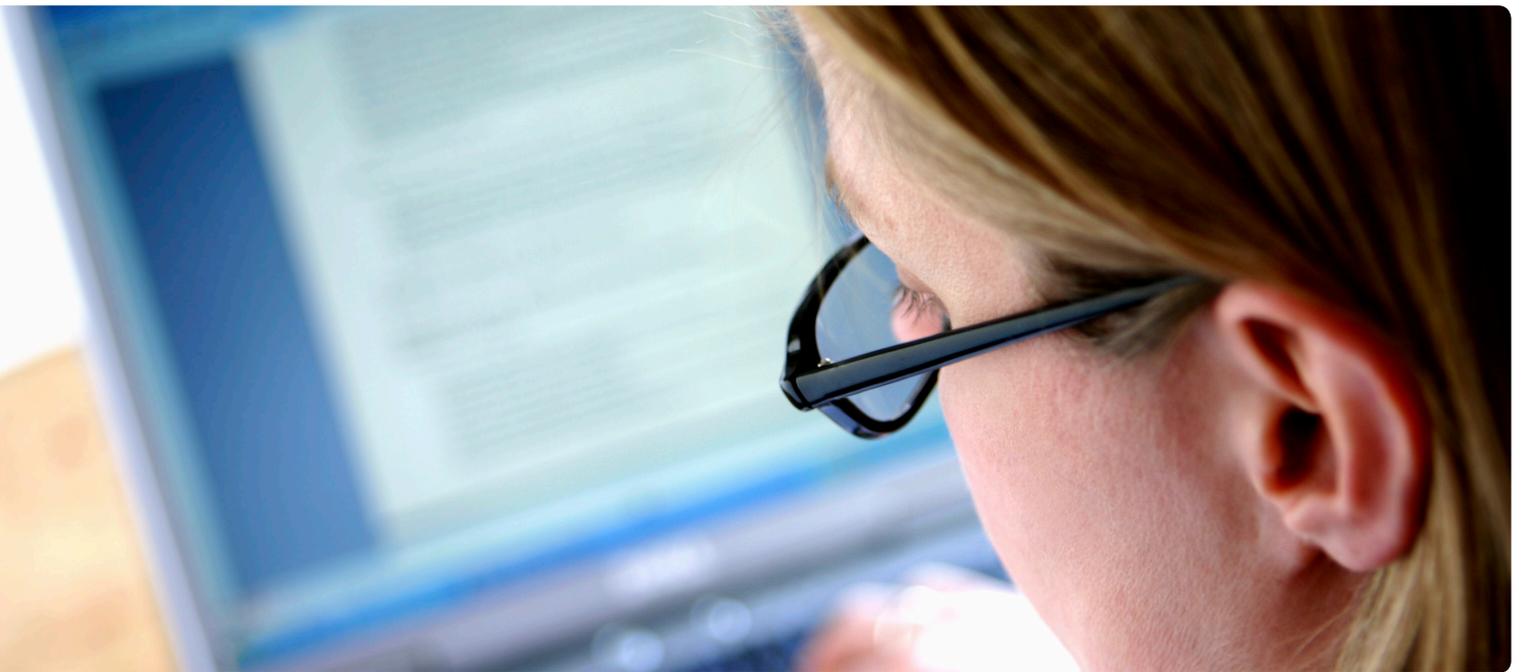


# Balancing Desktop Standardization with User Needs

Variety – The Spice of Life, The Bane of IT



## Abstract

Adopting a “corporate standard desktop” has undeniable benefits: it lowers overhead, reduces maintenance, and increases both stability and security.

But the two main client computer types that we’ve become accustomed to—laptops and desktops—aren’t the only game in town anymore. Now we’ve got a variety of virtual desktops, as well as published ones. Moreover, users today aren’t tied to a single client; they’re working from home, from the office, from hotels, and from airplanes.

That means that deploying a “corporate standard desktop” across the organization doesn’t work anymore. Users need different configuration settings depending on a variety of factors, from their current desktop to their current location to the time of day. This white paper explores how IT can balance the usefulness of desktop standardization with the real needs of today’s users.

## Introduction

### The “corporate standard desktop”

For years, one of IT’s best tricks for lowering overhead, reducing maintenance, and increasing both stability and security has been the “corporate standard desktop.” By getting every user on the same configuration, we eliminated a lot of the variables that caused downtime, protracted troubleshooting sessions, and related problems.

Of course, very few organizations are able to maintain a truly standard desktop in the face of dynamic business needs, changing user requirements, varying software editions and versions, and the steady trickle of new hardware entering the organization.

In fact, in the brave new world of “virtualized everything,” standardization has pretty much taken a flying leap off a tall building.

We need to be able to create configuration settings and then decide which computers will receive them using increasingly granular criteria.

## A configuration quiz: why standards don't work any more

Here's a quick quiz:

### Configuration quiz

You want to be sure that your users are all getting a particular configuration setting each time they log on. Perhaps it's a specific printer or drive mapping. You deploy a logon script to make it happen.

To which users and computers should that logon script be assigned?

- A. All users
- B. All computers
- C. All users and all computers
- D. None of the above
- E. Who the heck knows?

The correct answer is E. After all, it's unlikely that you want that printer mapped when someone logs onto a server console, right? And the folks working in the new remote office, or from home, don't need the printer mapping either. Users logging into a published client—say, one hosted in your Citrix infrastructure—need the printer, but not the drive. Users of your virtual desktop infrastructure (VDI) clients might not need either of the mappings.

That's the thing with "standards" these days: the exceptions start piling on pretty quickly. It isn't always obvious that there will be exceptions when you first get started with the standard, but they always crop up. It used to be that we all we had to worry about was a user's Windows version, their physical location, and maybe whether they were in a particular user group. We could handle those things with Group Policy. Now we've got to figure out if they're connecting via a slow VPN connection, or if their "client computer" is really a VDI session or even just a published application being served up by Citrix.

## What we need: an alternative to the static "standard desktop"

### Targeting configuration settings to desktops—physical, virtual, or published

The two main client computer types that we've become accustomed to—laptops and desktops—aren't the only game in town anymore. Now we've got a variety of virtual desktops, as well as published ones. It's crucial that our configuration tools be able to distinguish between them. If you're using Group Policy to deploy configuration settings, for example, differentiating between virtual and published desktops can be tricky, if not impossible.

Really, it's all about targeting. We need to be able to create configuration settings and then decide which computers will receive them—that is, which computers will be targeted—using increasingly granular criteria:

- What kind of client? Desktop? Portable? Tablet? Embedded? Virtual? Server? Published?
- What version of Windows?
- What connection type?
- What IP address range?
- What time of the day?
- What domain?
- What organization unit or group membership(s)?
- What site?

You might even want to create configurations that target based on aspects of the OS configuration, such as the presence of a specific file or registry key, or the setting of a registry value. The point is, you need to be able to target configuration settings in a much more dynamic, granular fashion than something like Group Policy offers.

### Limitations of native tools

Now, wait a minute. You're about to say that, through Windows Management Instrumentation (WMI), Group Policy can be pretty granular. True, if you happen to have an on-staff expert on the largely undocumented, inconsistently

implemented beast called WMI. And even then, WMI-based filters in Group Policy objects can be cumbersome to work with. For example, you can't reliably use a WMI filter to detect the presence of a particular file, because the CIM\_DataFile class that you'd need to use doesn't have incredibly awesome performance.

There are also the more-granular targeting criteria supported in Group Policy Preferences, right? Again, that's true—but those work only for the things in Group Policy Preferences, not globally across an entire Group Policy object. And, like WMI, Group Policy Preferences have a bit of a weak point. That weak point is reuse. Let's say you've come up with the WMI filter that beats all other WMI filters, and you've applied it to a Group Policy object. You've tested it, and it's finally working. Congrats! Now you want to use it again in another Group Policy object. Oh, too bad. You can't. Short of manually re-typing and testing everything, of course. That's because Group Policy—either in Preferences or through WMI filters—doesn't have a concept for creating a filter set that identifies a group of computers, and for letting you re-use that set.

Here's what would be better: the ability to create a named group of computers, and then define whatever crazy-granular criteria that identifies computers in that group. The group is thus dynamic: its members consist of any computer (or user—everything here applies to them, too) that happens to meet the stated criteria right then and there. Criteria like the following:

- All Citrix-published clients being used by members of the Sales user group who log on between 9 a.m. and 5 p.m.
- All physical computers connected to the company network in the Seattle office that have OurCorporateApp.exe on their local hard drive
- All virtual client computers running Windows XP that are being used by any user in the Operations organization unit who are logging on between 5 p.m. and 5 a.m. and who have the HKEY\_CURRENT\_

USER\SOFTWARE\Us\Permit key present in the registry

See? You want to be able to get really, really specific in defining these sets. Once a set is defined, you can then use it to target whatever configuration settings you like. Map drives. Map printers. Configure registries. Redirect folders. Apply Group Policy objects. Whatever. At least, those are all the things you should be able to do.

And yeah, you could probably hack all that out in a logon script. If you're a Grade A+ programmer. And if you have all the time in the world. And if you'll live forever to maintain the massive hunk of code you'll be writing. And if Microsoft doesn't discontinue whatever logon script language you were using. Then again, maybe massive logon scripts aren't the right answer.

#### **The virtual angle is crucial.**

One reason that it's so important to distinguish between virtual, physical, and published desktops lies in how they operate. For example, VDI-based desktops are often much more standards-based than someone's individual PC. VDI desktops may roll back to a "master" state each time someone logs off. That means it may not be appropriate to make a bunch of personalization changes each time a user logs on. Doing so might be pointless and simply take up time without serving any real need.

On the other hand, you might well have settings that you want to deploy only to those VDI desktops—and you want them deployed to every virtual desktop, regardless of other criteria. Being able to target to that level of granularity is crucial as we expand techniques and processes that have typically ever had to accommodate only laptop and desktop computers.

#### **The bottom line: make it about the user.**

At the end of the day, configuration control is primarily about users. We're either customizing the environment

Once a set of criteria is defined, you can use it to target whatever configuration settings you like. Map drives. Map printers. Configure registries.

Desktop Authority can bring more than 40 levels of targeting to Group Policy, giving you more than 3,000 configuration settings.

to make their jobs easier, or to protect them, or to provide better stability or security or whatever.

But users aren't tied to a single client anymore. They're everywhere—logging into virtual clients, using published applications, and carrying their laptops all over the world. They're working from home, from the office, from hotels, and from an airplane. In the office, they may need a certain printer and specific drive mappings; on a slow connection from an airplane, none of those are necessary. Unless they're using a virtual client, which isn't located on the airplane. Unless it's a virtual client that has access to confidential information, in which case maybe the printer mapping is a bad idea. Unless... well, you get the idea.

Building sets that identify these various scenarios—with an understanding of these different client scenarios—lets you custom-tailor every user experience to give users the best experience, the most secure experience, and the most stable experience.

#### **Finding the right tool**

##### **Please, not another ten consoles!**

Some folks will tell you that achieving this level of control, while being able to differentiate between physical, virtual, and published computers, will require a handful of different toolsets.

Great, more tools. More management consoles. More licenses to buy, more contracts to maintain, more icons to learn, and more moving parts to troubleshoot.

Look, just because virtual, physical, and published clients are different doesn't mean they're that different. Surely there's a way to manage all of your clients—regardless of how they're running—through a single solution? Some sort of master authority over configuration settings? Something that could, ideally, leverage all the settings you've already got in Group Policy and just make them more granularly-targeted?

Please?

#### **Get the configuration authority.**

With Desktop Authority Management Suite, administrators can proactively provision and manage a productive, secure and flexible Windows user environment that automates users' access to resources and applications. The suite includes three solutions: Desktop Authority Standard, MSI Studio and Privilege Manager.

Desktop Authority gives you all the power and granularity you need to build sets that identify users and computers based on whatever criteria you need—including whether a computer is physical, virtual, or published. Then assign configuration settings to those sets, precisely targeting exactly the necessary configuration at exactly the right time.

Everything's evaluated dynamically, meaning users' configurations can change as they move from place to place and client to client. Slow connection? Detected, and the appropriate configuration applied. Virtual client? Detected, and the right settings installed. Control printers, drives, registries, applications, and more—all without hand-coding a single logon script.

This is the "desired configuration management" that everyone's been raving about for years—and it's been hiding in Desktop Authority all along. Need to reconfigure the wallpaper on every virtual computer in the Denver office? No problem: click a few buttons in Desktop Authority's intuitive management console and it handles the rest. No scripts. No sweat. All in a single solution, managed from a single, simple graphical console.

Desktop Authority can even bring its more than 40 levels of targeting to Group Policy, giving you more than 3,000 configuration settings that you can push out with unprecedented dynamic precision.

So why not give it a try? You know you want to, and it doesn't cost a dime to look. Visit [www.quest.com/desktop-authority-management-suite](http://www.quest.com/desktop-authority-management-suite) for a free trial, guided tour, data sheets, and more.



### For More Information:

© 2012 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT,

DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

### About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit [www.dell.com](http://www.dell.com).

If you have any questions regarding your potential use of this material, contact:

### Dell Software

5 Polaris Way  
Aliso Viejo, CA 92656  
[www.dell.com](http://www.dell.com)

Refer to our Web site for regional and international office information.

