

JEREMY MOSKOWITZ

上海交通大学图书馆



E1276039

# Group Policy

Fundamentals,  
Security, and the  
Managed Desktop

**Second Edition**

# Group Policy

## Fundamentals, Security, and the Managed Desktop

Second Edition

Jeremy Moskowitz



John Wiley & Sons, Inc.

Acquisitions Editor: Mariann Barsolo  
Development Editor: Sara Barry  
Technical Editor: Alan Burchill  
Production Editor: Elizabeth Campbell  
Copy Editor: Liz Welch  
Editorial Manager: Pete Gaughan  
Production Manager: Tim Tate  
Vice President and Executive Group Publisher: Richard Swadley  
Vice President and Publisher: Neil Edde  
Book Designers: Judy Fung and Bill Gibson  
Compositor: Craig Woods, Happenstance Type-O-Rama  
Proofreader: Sarah Kaikini  
Indexer: Nancy Guenther  
Project Coordinator, Cover: Katherine Crocker  
Cover Designer: Ryan Sneed  
Cover Image: © Mehmet Hilmi Barcin / iStockPhoto

Copyright © 2013 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-118-28940-2

ISBN: 978-1-118-33392-1 (ePDF)

ISBN: 978-1-118-33174-3 (epub)

ISBN: 978-1-118-83356-2 (eMobi)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Limit of Liability/Disclaimer of Warranty:** The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit [www.wiley.com](http://www.wiley.com).

**Library of Congress Control Number:** 2012950506

**TRADEMARKS:** Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *Group Policy: Fundamentals, Security, and the Managed Desktop*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at [nedde@wiley.com](mailto:nedde@wiley.com). If you think you've found a technical error in this book, please visit <http://sybex.custhelp.com>. Customer feedback is critical to our efforts at Sybex.

Best regards,

A handwritten signature in black ink, appearing to read 'Neil Edde', with a stylized, flowing script.

Neil Edde  
Vice President and Publisher  
Sybex, an Imprint of Wiley



*To my wife, Laura, who always gives me the support I need.*

*—Jeremy*



# Acknowledgments

I want to thank Alan Burchill for taking on the not-so-glamorous job of Technical Editor. I'm really glad to have you on my team, helping me clean up the little messes I made during the writing process and taking on a heavy responsibility. Note: If there are still any technical problems with the book, blame me, not him. Alan was awesome.

I want to thank Sara Barry for taking my initial chapters and kneading them from a wad of dough into tasty pizza. And thanks go to Elizabeth Campbell, who has worked with me through every major project to completion for almost 12 years now. We joke that she's "been making Jeremy sound like Jeremy since 2001." And it's mostly true. Thank you.

Special thanks to my Sybex and Wiley compatriots: Peter Gaughan, Mariann Barsolo, Jay Lessandrini, Connor O'Brien, Rayna Erlick, Rebekah Worthman, and Neil Edde. Once again, your dedication to my book's success means so much to me. You take everything I create and deal with it so personally, and I really know that. Thank you, very sincerely.

Thanks to Jeff Hicks, PowerShell MVP, who helped me write the downloadable bonus chapter on Group Policy and PowerShell. Jeff, you did a smashing job, thank you.

Thanks to Brad Rudisail, who is a shining light of awesomeness; helping me out with both Group Policy and PolicyPak duties, left and right. Very glad you're on my team, and thanks for doing all the un-fun jobs you seem to actually find very fun.

Thank you to the Microsoft Group Policy team and the Group Policy MVPs who support me directly and indirectly and help me out whenever they can.

Thank you, Mark Minasi, for being a trusted friend, and a great inspiration to me personally and professionally.

Finally, I want to thank you. If you're holding this book, there's a good chance you've owned the previous edition or multiple previous editions. Thank you for your trust and for purchasing and repurchasing each edition of this book I work so hard to bring you each time.

When I meet you, the reader of this book, in person, it makes the hours and hours spent on a project like this vaporize away to a distant memory. Thank you for buying the book, joining me at my live events, joining me at GPAnswers.com, and for using my PolicyPak software. You all make me the best "me" I can be. Thanks.





# About the Author

**Jeremy Moskowitz**, Group Policy MVP, is the founder of GPanswers.com and PolicyPak Software (PolicyPak.com). He is a nationally recognized authority on Windows Server, Active Directory, Group Policy and Windows management. He is one of fewer than a dozen Microsoft MVPs in Group Policy. His GPanswers.com is ranked by Computerworld as a "Top 20 Resource for Microsoft IT Professionals." Jeremy contributes to Microsoft Springboard series, *Windows IT Pro Magazine*, and *Redmond Magazine*. Jeremy is a sought-after speaker and trainer at many industry conferences and his training workshops helps thousands of administrators every year do more with Group Policy. Contact Jeremy by visiting GPanswers.com or PolicyPak.com.

# About the Contributors

**Jeffery Hicks** (MCSE, MCSA, MCT) is a Microsoft PowerShell MVP with 20 years of diverse IT experience. He works today as an independent author, trainer, and consultant. Jeff is a columnist for MCPMag.com and a regular contributor to the Petri IT KnowledgeBase. His latest books are *PowerShell in Depth: An Administrators Guide* (Manning, 2012) and *Learn PowerShell 3 in a Month of Lunches* (Manning, 2012). You can follow Jeff at [jdhitolutions.com/blog](http://jdhitolutions.com/blog) and [twitter.com/jeffhicks](https://twitter.com/jeffhicks).

**Alan Burchill** works as a Senior Consultant for Avanade based in Brisbane, Australia. He is a Microsoft Valuable Professional in the area of Group Policy and regularly blogs about Group Policy topics at his website called Group Policy Central at [www.grouppolicy.biz](http://www.grouppolicy.biz). You can reach him via Twitter at [@alanburchill](https://twitter.com/alanburchill).

# Introduction

The era of Windows 8 is here. And, here's the good and bad news (which is the same news): Besides that whole Start Screen/Start Menu business, Windows 8 is not radically different from its Windows 7 sibling.

This awareness is a dual-edged sword. On the one hand, you could say to yourself, "Awesome! If I'm already an expert at Windows 7 and Group Policy, there's not a huge hill to climb!" And that would be true. On the other hand, it's also true that because Windows 8 didn't shake things up too much, there's no "super killer must-haves" about Windows 8 with regard to Group Policy "guts."

In a way, I really like the dual-edged sword. I like that there is a variety of new goodies for Windows 8, some interesting updates, but not a radical head-spinning change. I like the fact that what is already working in practice doesn't change that much. I like knowing that the time already invested in getting smarter in Group Policy isn't for nothing, and you and I won't have to re-learn everything we ever knew all over again.

In short, I'm happy with Windows 8's updates with regard to Group Policy. Group Policy has been around since Windows 2000 and continues on through Windows XP, Windows Vista, all the Windows Server operating systems and now on to Windows 8 Client and Windows Server 2012.

That's an amazing run for one technology. What other technology has been around for almost 12 years and is still *gaining* in popularity? Its increased popularity and widespread use has grown, year after year. And the underlying technology—both at its core and what it controls—has received an infusion of new technologies to keep it not only still relevant, but indeed, *central* to any Active Directory administrator's tool belt of required knowledge.

Group Policy and Active Directory go hand in hand. If you have Active Directory, you get Group Policy.

If you're new to Group Policy, here's the inside scoop. Group Policy has one goal: to make your administrative life easier. Instead of running around from machine to machine, tweaking a setting here or installing some software there, you'll have ultimate control from on high.

Like Zeus himself, controlling the many aspects of the mortal world below, you will have the ability, via Group Policy, to dictate specific settings pertaining to how you want your users and computers to operate. You'll be able to shape your network's destiny. You'll have the power. But you need to know how to tap into this power and what can be powered.

In this introduction and throughout the first several chapters, I'll describe just what Group Policy is all about and give you an idea of its tremendous power. Then, as your skills grow, chapter by chapter, we'll build on what you've already learned and help you do more with Group Policy, troubleshoot it, and implement some of its most powerful features.

## Group Policy Defined

If we take a step back and try to analyze the term *Group Policy*, it's easy to become confused. When I first heard the term, I didn't know what to make of it.

I asked myself, "Are we applying 'policy' to 'groups'? Is this some sort of old-school NT 4 System Policy applied to Active Directory groups?"

Turns out, "Group Policy" as a name isn't, well, excellent. That's because, at cocktail parties, I have a hard time telling the person next to me what I teach and write about.

If I said something like "I teach databases," he would cheerfully go back to his scotch and soda and leave me alone. But because I say, "I teach Group Policy to smart people looking to get smarter," he (unfortunately) wants to know more. He'll say something like "What does that mean? I've never heard of Group Policy before." And while I love talking about Group Policy with you, my friendly IT geeks, at a cocktail party full of stuffed shirts, I just want to get another canapé.

So, the name "Group Policy" can be kind of confusing, but it's also intriguing. Microsoft's perspective is that the name "Group Policy" is derived from the fact that you are "grouping together policy settings." I don't really love the name Group Policy—but it's the name we have, so that's what it's called. As Juliet might say, "What's in a name? That which we call a rose by any other name would smell as sweet," (*Romeo and Juliet*, II, ii, 43–44).

Group Policy is, in essence, rules that are applied and enforced at multiple levels of Active Directory. Policy settings you dictate must be adhered to by your users and computers. This provides great power and efficiency when manipulating client systems.

Instead of running around from machine to machine, you're in charge (not your users).

When going through the examples in this book, you will play the various parts of the end user, the OU administrator, the domain administrator, and the enterprise administrator. Your mission is to create and define Group Policy using Active Directory and witness it being automatically enforced. What you say goes! With Group Policy, you can set policies that dictate that users quit messing with their machines. You can dictate what software will be deployed. You can determine how much disk space users can use. You can do pretty much whatever you want—it is up to you. With Group Policy, you hold all the power. That's the good news.

And this magical power only works on Windows 2000 or later machines. That includes Windows 2000, Windows XP, Windows Server 2003 (as a client), Windows Vista, Windows Server 2008 and 2008 R2 (as a client), Windows 7, and of course, Windows 8 and Windows Server 2012.

This shouldn't be a problem, since you've expunged all the Windows 95, Windows 98, or Windows NT workstations or servers. Hey, it is 2013 (or maybe later!), after all!

I'll likely say this again in multiple places, but I want to get one "big ol' misconception" out of the way right here, right in the introduction. The Group Policy infrastructure does not care what mode your domain is in. If you have only one type of Domain Controller, or a mixture of Domain Controllers, 100 percent of everything we cover in this book is valid.

Said another way, even if your domain level is the oldest-of-the-old Windows 2000 mixed mode, you're still 100 percent covered here. Group Policy is all about the client (the target) operating system, and not the Domain Controllers or domain modes.

If the range of control scares you, don't be afraid! It just means more power to hold over your environment. You'll quickly learn how to wisely use this newfound power to reign over your subjects, er, users.

## Group Policy vs. Group Policy Objects vs. Group Policy Preferences

Before we go headlong into Group Policy theory, let's get some terminology and vocabulary out of the way:

- *Group Policy* is the concept that, from on high, you can do all this “stuff” to your client machines.
- A *policy setting* is just one individual setting that you can use to perform some specific action.
- *Group Policy Objects* (GPOs) are the “nuts and bolts” contained within Active Directory Domain Controllers, and each can contain anywhere from one to a zillion individual policy settings.
- The *Group Policy Preferences* is a newer add-on to the existing set of the “original” Group Policy many have come to know and love. Group Policy Preferences (sometimes shortened to GPPrefs, or GPP) don't act quite the same as their original cousins. We'll cover the Group Policy Preferences in detail in Chapter 5.
- *Preference item* is a way to describe one “Group Policy Preferences directive.” It's like a “policy setting,” but for the Group Policy Preferences.

It's my goal that after you work through this book, you'll be able to jump up on your desk one day and use all the vocabulary at once. Like this: “Hey! *Group Policy* isn't applying to our client machines! Perhaps a *policy setting* is misconfigured. Or, maybe one of our *Group Policy Objects* has gone belly up! Heck, maybe one of the *preference items* is misconfigured. I'd better read about what's going on in Chapter 7, “Troubleshooting Group Policy.”

This terminology can be a little confusing—considering that each term includes the word *policy*. In this text, however, I've tried especially hard to use the correct nomenclature for what I'm describing. If you get confused, just come back here to refresh your brain about the definitions.



Note that there is never a time to use the phrase “Group Policies.” Those two words together shouldn't exist. If you're talking about “multiple GPOs” or “multiple policy settings” or “policy settings vs. preference items,” these are the preferred phrases to use, and never “Group Policies.”

## Where Group Policy Applies

Group Policy can be applied to many machines at once using Active Directory, or it can be applied when you walk up to a specific machine. For the most part, in this book I'll focus on using Group Policy within an Active Directory environment, where it affects the most machines.

A percentage of the settings explored and discussed in this book are available to member or stand-alone Windows machines—which can either participate or not participate in an Active Directory environment.

However, the Folder Redirection settings (discussed in Chapter 10) and the Software Distribution settings (discussed in Chapter 11) are not available to stand-alone machines (that is, computers that are not participating in an Active Directory domain). In some cases, I will pay particular attention to non-Active Directory environments. However, most of the book deals with the more common case; that is, we'll explore the implications of deploying Group Policy in an Active Directory environment.

## The “Too Many Operating Systems” Problem

If we line up all the operating systems that you (a savvy IT person) might have in your corporate world, we would likely find one or more of the following (presented here in date-release order):

- Windows 2000 (Workstation and Server), RTM through SP4
- Windows 2003 Server, RTM through SP2
- Windows XP, RTM through SP3
- Windows Vista, RTM through SP2
- Windows Server 2008, RTM (known as SP1, actually) through SP2
- Windows 7 RTM, through SP1 Windows Server 2008 R2, through SP1
- Windows 8 client, RTM
- Windows Server 2012, RTM

For the love of Pete (whoever Pete is), that's a *lot* of potential operating systems. Okay, okay—perhaps you don't have *all* of them. You likely don't have any more Windows 2000 (or maybe you *do*, tucked in a back room somewhere, quietly processing something or other).

The point, however, is that Group Policy can apply to *all* of these systems. Under most circumstances, “old stuff” will work correctly on newer machines. That is, generally, something that can affect, say, an XP machine will also (generally) continue to affect a Windows 8 machine.

With that in mind, here's an example of what I'm *not* going to do. I'm *not* going to show you an example of something in the book, then say something like “... and this example is valid for Windows XP, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows 8, and Windows Server 2012.”

My head (and yours) will just explode if I do that and you need to read that each time.

So, here's what I *am* going to do. You'll read my discussion about something, then I'll say something like "... and this example is valid for Windows XP and later." That would mean that the concept, for example, policy setting, should work A-OK for XP and later machines (all the way to Windows 8 and also usually for servers, like Windows Server 2012, too). Similarly, if I say "... and this is valid for Windows Vista and later," that means you'll be golden if the target machine is Windows Vista and later (including Server 2008, Server 2008 R2, Windows 7, Windows 8, and Windows Server 2012).

Of course, there are a handful of exceptions: things that only work on one particular operating system in a possibly peculiar way. For instance, there are a handful of Windows Vista-only settings that aren't valid for Windows 7 and Windows 8 (or Windows Server 2008 R2 and Windows Server 2012) machines. And, on rare occasions, a particular service pack of a particular operating system is affected by a setting, where it wasn't previously available. Again, I'll strive for clarity regarding the exceptions—but the good news is, those are few and far between.

If you get lost, here's a quick cheat sheet to help you remember "which machines act alike":

- Windows 2000 Workstation and Windows Server
- Windows 2003 Server and Windows XP
- Windows Server 2008 and Windows Vista
- Windows 7 and Windows Server 2008 R2
- Windows 8 and Windows Server 2012

Just to be even more specific, Windows 7, Windows 8, Windows Server 2008 R2, and Windows Server 2012 are ludicrously close brothers. They look alike, throw the same temper tantrums, and enjoy the same kinds of movies. But they're not twins. They are different, but, in most cases, they're super-duper similar.

For this edition of the book, we decided to make a conscious choice about how to present Group Policy. Most of the walkthroughs, examples, and screen shots in the book will be of Windows 8 and Windows Server 2012.

Since Windows XP is on the way out, we decided to rein in the amount of Windows XP examples this time and give you a leaner, meaner book. Yes, there is still a lot of Windows XP details and "need to knows" in this book. Discussions on XP are not gone from these pages. However, where something became so outmoded that it needed the heave-ho, I will refer you to the previous edition of the book, which goes into excruciating detail on Windows XP.

But I do want to be super-clear about something: I am also specifically going to note and talk about the differences between the various operating systems. For instance, I'll definitely be expressing some concepts as originally found in Windows 2000 and also Windows XP—things that were originally in the operating systems' behaviors, but are absent or changed now.

I like to talk about the "old school" stuff sometimes, because I find it helps explain why Windows does some things today that seem, well, odd or confusing. If I explain the older operating systems, for example, Windows 2000 and Windows XP, it's actually *easier* to understand modern Windows.



A quick word about Windows Vista. When Vista was released, Microsoft released sales figures saying that they sold millions and millions of Vista licenses. But ask a hundred IT shops, “Did you deploy Vista?” and you won’t get much response. I honestly don’t know what to believe other than what I see with my two eyes, and what people *tell* me. What I *see* and what people *tell* me is that they basically “skipped Vista.” Many organizations bypassed Vista and used some mix of Windows XP in conjunction with Windows 7. So, as I write this, most IT shops I know of have a lot of Windows XP in house today and are migrating away from Windows XP and toward Windows 7 and now toward Windows 8.

So, of all the operating systems in this book, the one I’ll be spending the least amount of time on is Vista itself.

But we also cannot deny the existence of Windows Vista.

Yes, friends. Vista happened.

It turns out that even though Microsoft “didn’t quite get the taste right” with regard to Windows Vista, the individual ingredients continue to be the base of our Windows soup going forward. So, that means Windows 7 and its sibling Windows 8 is, more or less, a minor upgrade from Vista. And pretty much everything that was once valid for Vista is *also* valid for Windows 7 and Windows 8. Therefore, you’ll see me write a lot about “... and this works for Windows Vista and later” or in some places, like table listings, you’ll see “Valid for Vista+”—meaning that whatever I’m referencing will work on Vista (if you have it), but it will also work on Windows 7 and almost always, also Windows 8.

## This Book and Beyond

Group Policy is a big concept with some big power. This book is intended to help you get a handle on this new power to gain control over your environment and to make your day-to-day administration easier. It’s filled with practical, hands-on examples of Group Policy usage and troubleshooting. It is my hope that you enjoy this book and learn from my experiences, so you can successfully deploy Group Policy and manage your desktops to better control your network. I’m honored to have you aboard for the ride, and I hope you get as much out of Group Policy as I do from writing and speaking about it in my hands-on workshops.

As you read this book, it’s natural to have questions about Group Policy or managing your desktops. To form a community around Group Policy, I have a popular community forum that can be found at [www.GPanswers.com](http://www.GPanswers.com).

I encourage you to visit the website and post your questions to the community forum or peruse the other resources that will be constantly renewed and available for download. For instance, in addition to the forum at [www.GPanswers.com](http://www.GPanswers.com), you’ll find:

- Two extra downloadable chapters from this newest edition of the book
- Full downloadable PowerShell scripts from one of those downloadable chapters
- One older reference chapter (on ADM files) in case you need it
- Tips and tricks
- A third-party Group Policy Solutions Guide, and lots, lots more!