

SYBEX Bonus Chapter

# **Group Policy, Profiles, and IntelliMirror for Windows<sup>®</sup> 2003, Windows<sup>®</sup> XP, and Windows<sup>®</sup> 2000 (Mark Minasi Windows<sup>®</sup> Administrator Library) Jeremy Moskowitz**

## **Web Chapter 3: Restricted Group Tables**

Copyright © 2004 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

ISBN: 0-7821-4298-2

SYBEX and the SYBEX logo are either registered trademarks or trademarks of SYBEX Inc. in the USA and other countries.

TRADEMARKS: Sybex has attempted throughout this book to distinguish proprietary trademarks from descriptive terms by following the capitalization style used by the manufacturer. Copyrights and trademarks of all products and services listed or described herein are property of their respective owners and companies. All rules and laws pertaining to said copyrights and trademarks are inferred.

This document may contain images, text, trademarks, logos, and/or other material owned by third parties. All rights reserved. Such material may not be copied, distributed, transmitted, or stored without the express, prior, written consent of the owner.

The author and publisher have made their best efforts to prepare this book, and the content is based upon final release software whenever possible. Portions of the manuscript may be based upon pre-release versions supplied by software manufacturers. The author and the publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book.

Sybex Inc.  
1151 Marina Village Parkway  
Alameda, CA 94501  
U.S.A.  
Phone: 510-523-8233  
[www.sybex.com](http://www.sybex.com)

# 3

## Restricted Groups Tables

If you worked through the examples in Chapter 6, you got to do a little experimenting with the Restricted Groups functionality within Group Policy. As a quick refresher, Restricted Groups allows you to control the following:

- The membership of security groups that you create in Active Directory
- The security group membership on groups created on member machines (workstations or servers)
- The security groups that are nested within each other

To get started with Restricted Groups, first create a new GPO. Then follow these steps:

1. Traverse to Computer Configuration > Windows Settings > Security Settings > Restricted Groups.
2. Right-click the Restricted Groups node and choose “Add Group” from the shortcut menu to open the “Add Group” dialog box.



You're concerned with the "Members of this group" and "This group is a member of" sections. At this point you can add users or groups to either section. (That's right. You can add users to the "This group is a member of" section.) As I said in Chapter 6, you don't actually have to tell this section about a group. You can lie to it and tell it about a user. When you do so, that user is ensured of being in the group.

I encourage you to first try the exercises in Chapter 6 before experimenting. Different domain modes allow for different levels of group nesting. And you can nest a lot of different types, depending on whether you're working with local accounts (on workstations, SQL servers, and so on) or with accounts you can "browse" to within Active Directory.

## How to Use These Tables

These tables explain the possibilities within Restricted Groups. There are three variables:

- Which function am I using? ("Members of this group" or "This group is a member of")
- What is the domain mode?
- What kind of account am I trying to manipulate?(local group, local user, Active Directory group, Active Directory user)

To use this chapter and these tables, first note the title of the section. For example, the next section is "Manipulating Active Directory Groups (and Active Directory Users) via Restricted Groups." That section contains two tables: Members of This Group and This Group Is a Member Of. Select a table, read the first column to get the first half of the sentence, and then read the first row to complete the sentence.

You can determine many outcomes from each table. For example, from Table 3.1, you can answer several questions:

- Can I use Restricted Groups to force a universal group into a universal group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)? Answer: Yes.
- Can I use Restricted Groups to force a domain user into a domain local group when the domain mode is Windows 2000 (Mixed)? Answer: No.
- Can I use Restricted Groups to force a domain local group into a universal group when the domain mode is Windows 2000 (Mixed)? Answer: Not possible.



The original material for these tables comes courtesy of Microsoft. Although I'm sure Microsoft made every effort to ensure that the data in the tables is sound, I encourage you to verify the scenarios you want to use in a test lab before rolling them out into production.

# Manipulating Active Directory Groups (and Active Directory Users) via Restricted Groups

**TABLE 3.1** Members of This Group

	into a universal group when the domain mode is Windows 2000 (Mixed)?	into a universal group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?	into a global group when the domain mode is Windows 2000 (Mixed)?	into a global group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?	into a domain local group when the domain mode is Windows 2000 (Mixed)?	into a domain local group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?
Can I use Restricted Groups to force a universal group...	Not possible	Yes	Not possible	No	Not possible	Yes
Can I use Restricted Groups to force a global group...	Not possible	Yes	No	Yes	Yes	Yes
Can I use Restricted Groups to force a domain local group...	Not possible	No	No	No	No	Yes
Can I use Restricted Groups to force a Domain User...	Not possible	Yes	Yes	Yes	Yes	Yes

**TABLE 3.2** This Group Is a Member Of

	into a universal group when the domain mode is Windows 2000 (Mixed)?	into a universal group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?	into a global group when the domain mode is Windows 2000 (Mixed)?	into a global group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?	into a domain local group when the domain mode is Windows 2000 (Mixed)?	into a domain local group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?
Can I use Restricted Groups to force a universal group...	Not possible	Yes	Not possible	No	Not possible	Yes
Can I use Restricted Groups to force a global group...	Not possible	Yes	No	Yes	Yes	Yes
Can I use Restricted Groups to force a domain local group...	Not possible	No	No	No	No	Yes
Can I use Restricted Groups to force a Domain User...	Not possible	Yes	Yes	Yes	Yes	Yes



Remember that you can "lie" to the "This group is a member of" section and supply a user name instead of supplying a group. (Not that you necessarily should.)

# Manipulating Local Groups (and Local Users) via Restricted Groups



Table 3.3 was produced with Windows XP/SP2 (beta). Be sure to verify your results in the test lab with your target operating system before rolling out into production.

**TABLE 3.3** Members of This Group

	into a local group when the domain mode is Windows 2000 (Mixed)?	into a local group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?
Can I use Restricted Groups to force a universal group...	Not possible	Yes
Can I use Restricted Groups to force a global group...	Yes	Yes
Can I use Restricted Groups to force a local group...	No	No
Can I use Restricted Groups to force a local user...	Yes	Yes

**TABLE 3.4** This Group Is a Member Of

	to be a member of a local group when the domain mode is Windows 2000 (Mixed)?	to be a member of a universal group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?
Can I use Restricted Groups to force a universal group...	Not possible	No
Can I use Restricted Groups to force a global group...	Yes	No
Can I use Restricted Groups to force a local group...	No	No

**TABLE 3.4** This Group Is a Member Of *(continued)*

	<b>to be a member of a local group when the domain mode is Windows 2000 (Mixed)?</b>	<b>to be a member of a universal group when the domain mode is Windows 2000 Native or Windows 2003 (Full Functional)?</b>
Can I use Restricted Groups to force a local user...	Yes	Yes
Can I use Restricted Groups to force a domain local group...	Yes	Yes
Can I use Restricted Groups to force a domain user...	Yes (should be included in Windows XP with SP2)	Yes (should be included in Windows XP with SP2)



Remember that you can "lie" to the "This group is a member of" function and supply a user name instead of supplying a group. (Not that you necessarily should.)