Nightmare on Delegation Street with Native Active Directory Tools

Written By Quest Software

QUEST SOFTWARE®
Simplicity At Work®

Contents

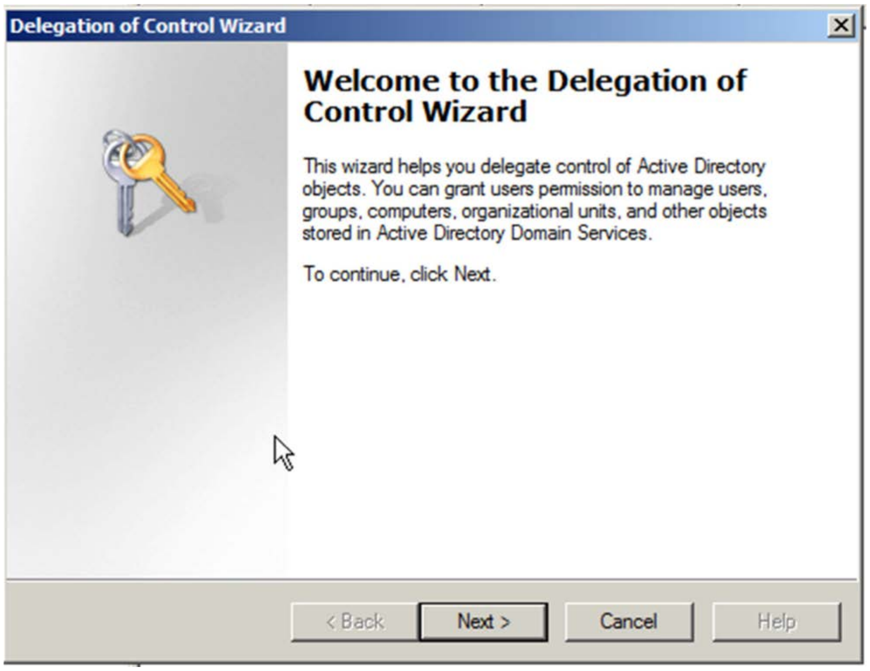
Abstract

Delegating Active Directory permissions – and managing and reporting on those delegations – is a nightmare. If you're using native tools, that is. With the right tools, the job is easy. Read on to learn how to put your AD delegation nightmares to rest, forever.

Introduction

It’s nighttime. The data center is dark, and just a bit spooky. The hum of powerful HVAC units takes on an almost sinister tone. You’re not really here; you’re at home, in bed. Asleep. But is this a dream?

You’re standing in front of a server rack, logged into the console of a domain controller. Active Directory Users and Computers is open before you, and you see a familiar wizard:



Delegation of Control Wizard

Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

From all around you, you can hear the unsettling sound of metal scraping on metal, as if clawed fingers were being raked across the backs of the server racks. A harsh voice floats around the room: “Make sure the administrative assistants in Denver can reset passwords for the users there… Make sure the help desk can change user attributes in the directory… Give Human Resources the ability to update departmental and organizational information in the directory… Delegate! Delegate! Delegate!”

You furiously start clicking buttons, checking boxes, and typing organizational unit names. Next, Next, Finish! Next, Next, Next, Finish!

As you complete delegation after delegation, the voice comes back, even softer and more sinister: “Now take away that Denver assistant’s abilities…. Restrict Human Resources to just the people in the main office…. Who can update organizational information now?”

Your fingers stop, twitching above the keyboard. Your mouse hand is shaking. You can’t do those things with the Delegation of Control Wizard. It’s for delegating control, not for reporting on delegation or changing delegations. The voice’s evil laughter fills your ears, and you feel a thin sliver of metal sliding down your bare neck…

You wake up, your sheets soaked in sweat. Your mouse hand is still trembling. And there’s a thin cut on the back of your neck.

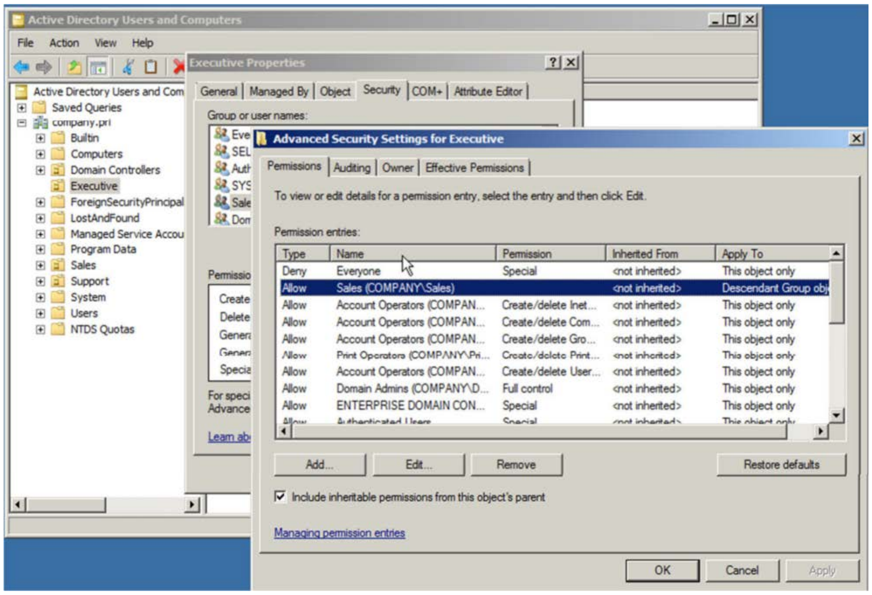
Delegation: Seemed Like a Good Idea at the Time

Delegation Is Easy

Active Directory has great support for fine-grained permissions, and Microsoft's intent all along was for you to be able to dole out just the permissions people needed over specific portions of the directory. Delegation was intended to be a way for certain tasks to be taken off of IT's back and put into the hands of people throughout the organization. Whatever tasks you need to delegate – keeping directory attributes updated, unlocking accounts, resetting passwords – can be delegated. And the Delegation of Control (DoC) Wizard makes it pretty easy to set up delegation, by offering pre-packaged sets of permissions that you can drop onto an organizational unit (OU).

But Maintenance Is Difficult

The problem is in maintaining that delegation over time. The native Active Directory tools don't provide any way of seeing who has been delegated what, apart from the native, one-object-at-a-time permissions dialog:



To view or edit details for a permission entry, select the entry and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Deny	Everyone	Special	<not inherited>	This object only
Allow	Sales (COMPANY\Sales)		<not inherited>	Descendant Group obj
Allow	Account Operators (COMPAN...	Create/delete Inet...	<not inherited>	This object only
Allow	Account Operators (COMPAN...	Create/delete Com...	<not inherited>	This object only
Allow	Account Operators (COMPAN...	Create/delete Gro...	<not inherited>	This object only
Allow	Print Operators (COMPANY\Pri...	Create/delete Print...	<not inherited>	This object only
Allow	Account Operators (COMPAN...	Create/delete User...	<not inherited>	This object only
Allow	Domain Admins (COMPANY\D...	Full control	<not inherited>	This object only
Allow	ENTERPRISE DOMAIN CON...	Special	<not inherited>	This object only
Allow	Authenticated Users	Special	<not inherited>	This object only

☑ Include inheritable permissions from this object's parent

Those permissions are complex and difficult to read from within the dialog. You have to perform numerous interactions: What permission has been applied? What does it apply to? Will it inherit to child containers? You have to dig in through three or four levels of dialogs to see exactly what was delegated – and it's incredibly easy to misunderstand a checkbox, click the wrong one, and delegate too many permissions.

Worse, there's no centralized reporting whatsoever. The native tools don't let you see "what permissions have been delegated to HR, and where?" You can't see "which OUs have permissions other than the defaults?" It's all a manual process of dialog box spelunking. Sure, you could write scripts, but those scripts are going to do nothing more than manually scan every single object and report on the permissions. That can be a glut of data, and unfortunately Microsoft hasn't yet created the interfaces that such a script would actually need to run efficiently and effectively.

Reporting on permissions isn't the only problem: Setting up new permissions is harder than it should be, the DoC Wizard notwithstanding. Aside from its few prepackaged sets of permissions, there are no other sets that can be quickly delegated. Sure, you can delegate a "custom task," but that just dumps you into the same confusing cycle of "what are you delegating," "to whom are you delegating," "how will it inherit," "what will it apply to" and so forth – and you'd better know the under-the-hood directory class names that you want to work with, because that's what the Wizard is going to show you.

It's no use drinking energy drinks and coffee all night. Eventually, you're going to fall asleep, and the nightmare will begin again. The good news is that you'll probably be fine when you wake up… and then you can go to work and live the delegation nightmare for real.

Banishing the Nightmare

What’s needed is a reset on the way you think about AD delegation. Frankly, a better-designed user interface – one intended for permissions management – would go a long way toward solving the problem, as would some permissions-specific tools that don’t require digging into deeply-nested dialog boxes for every tidbit of information.

What about color-coding permissions, so that inherited, default, and explicit permissions are visibly differentiated? That would be a huge help; rather than looking at rows of checkboxes, or script- produced “Read-Write-Modify-Traverse” output, you could look at something visually designed to be meaningful to a human being instead of a machine. You could easily pick out inherited permissions, direct permissions, and so forth, and start modifying them as needed.

What about templates for permissions so you could define sets of permissions for specific tasks and then simply assign the template to the users who need it? Those templates could even be self-healing, meaning they’re constantly checked against the actual state of Active Directory and that an alert is generated if differences are found.

Templates would be an awesome idea. They’d really be an ideological extension of the DoC Wizard’s “Custom Tasks.” Only templates could be saved, making them easy to re-use in the future. Someone new joins the organization and needs a specific set of permissions? Just slap a template on ‘em, and the job is done. And that self-healing aspect would be especially useful, because if anyone else went directly into the directory and started mucking with things, you’d get an immediate alert and be able to re-apply the template to put things back the way they’re supposed to be.

Imagine those templates in an organization dealing with industry and legislative compliance! Your auditors would be delighted. Just show them the templates, and show them that the system hadn’t generated any template non-compliance alerts. Let them spot-check a few permissions manually (it’s what they’re paid to do), and they can trundle away, satisfied that everything is and has been as it should be.

Sound like a happy, pleasant dream?

A Delegation Dream Come True

There's really a way to make this happen, and it's called Quest Active Administrator.

With it, you create Active Templates that designate what is being delegated, who you're delegating to, and where in the directory the delegation applies. You can manage that delegation any time you want to by simply modifying the template; it updates Active Directory automatically. Changes made directly to the directory's permissions are caught, used to generate notifications, and then reset to the template's settings.

This approach makes viewing "who's been delegated what" as simple as looking at your templates. You can also use an intuitive, security-centric view of the directory to see current permissions – and color-coding distinguishes default permissions, inherited permissions, explicit permissions, and permissions assigned via an Active Template. Looking for explicitly-assigned permissions so that you can clean them up? No problem: they show up in a unique color and are easy to pick out of the user interface.

Because Active Administrator is designed for security, modifying permissions and even delegating control is easier and more intuitive. Create reports, reset permissions to their defaults, filter out default and inherited permissions, and do whatever else you might need – all with a few mouse clicks.

And this just scratches the surface of what Active Administrator can do for your directory. It also offers superior Group Policy management, robust AD auditing and recovery, role-based access control systems, and much more. You can even play with it in a live, online TestDrive – just visit www.quest.com/active-administrator. Or you can download a free trial and play with it in your own lab. You'll be impressed. You'll sleep easier, too.

The information in this document is provided in connection with Quest 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 Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST 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 QUEST 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 QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest 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. Quest does not make any commitment to update the information contained in this document.

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

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

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

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BridgeAccess, BridgeAutoEscalate, BridgeSearch, BridgeTrak, BusinessInsight, ChangeAuditor, ChangeManager, Defender, DeployDirector, Desktop Authority, DirectoryAnalyzer, DirectoryTroubleshooter, DS Analyzer, DS Expert, Foglight, GPOADmin, Help Desk Authority, Imceda, IntelliProfile, InTrust, Invirtus, iToken, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogADmin, MessageStats, Monosphere, MultSess, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Point,Click,Done!, PowerGUI, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportADmin, RestoreADmin, ScriptLogic, Security Lifecycle Map, SelfServiceADmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer, vRanger, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, WebDefender, Webthority, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Updated—SEPTEMBER 2012

About Quest Software, Inc.

Established in 1987, Quest Software (Nasdaq: QSFT) provides simple and innovative IT management solutions that enable more than 100,000 global customers to save time and money across physical and virtual environments. Quest products solve complex IT challenges ranging from database management, data protection, identity and access management, monitoring, user workspace management to Windows management. For more information, **visit www.quest.com.**

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)
If you are located outside North America, you can find your local office information on our Web site.

EMAIL sales@quest.com

MAIL Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service.
Visit SupportLink at https://support.quest.com.

SupportLink gives users of Quest Software products the ability to:

Search Quest's online Knowledgebase
Download the latest releases, documentation and patches for Quest products
Log support cases
Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information and policies and procedures.

WPW-NightmareonDelegationStreetWNativeActiveDirectoryTools-US-TG-20120831