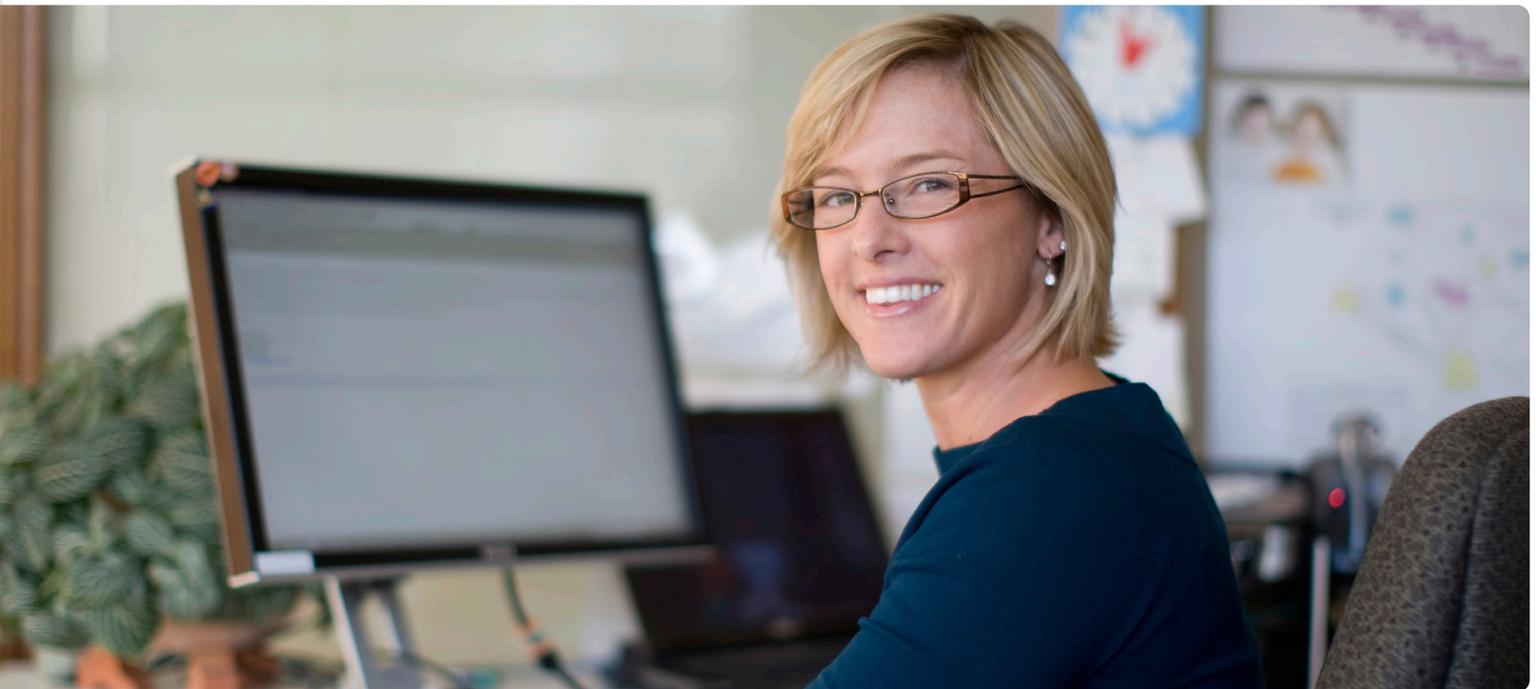


Killing Administrator Rights

Solving Three Problems by Eliminating Administrative Rights

Written by Greg Shields, Senior Partner and Principal Technologist, Concentrated Technology



Introduction

It's high time we killed administrator.

Now, before you run for the authorities, we're not talking about killing *the* administrator. That would be you, and that would be wrong. Rather, it's time we eliminated the *role* of administrator from our Windows servers and desktops.

Why? Inside Microsoft Windows, the notion of administrator and administrator rights was never well designed in the first place. With the initial design, we've long been suffering under what amounts to a binary view of privileges: *Do you have administrator rights or don't you* have been the only options at our disposal.

Yet simply killing off administrator doesn't solve the problem. Something must fill the hole its death leaves behind. In its place, IT dreams of a more granular approach to privilege management, one that aligns the actions users want to accomplish with those that you've specifically permitted.

Eliminating "the administrator" from administrator rights solves three big problems that have plagued Windows administration for years. First, moving rights management away from its historical person-based approach brings us closer to the goal we've been dreaming of: least privilege. **Problem number one** is figuring out how to get there.

Getting to least privilege requires a new approach, along with a new set of tools. That's why solving the second problem starts by flushing the binary notion of administrator versus non-administrator from our minds. Doing so frees us to think granularly about how users can be mapped to actions based on policies. **Problem number two** is all about getting that granularity.

As you can imagine, lots of granularity means lots of potential actions to catalog. Least privilege won't build itself. That's why the third problem's resolution requires some way to share

those rules that work best. **Problem number three** is in finding those rules that work.

Let's take a closer look at these three big problems that get solved with administrator's demise. With a little effort and the right tools, you'll find that making the move to granular privilege management has never seemed so easy.

Problem #1: Getting to least privilege

Don is a software developer in a mid-sized company, but his company isn't in the software business. They sell tires. While most of his co-workers deal with the day-to-day activities associated with tires and their sale, Don's position is unique. He's tasked with creating software solutions that enable the others to do their jobs.

There's just one problem. Don's company places a high value on security. So high, in fact, that very few people are granted administrator rights. Even Don can't get them. Getting anything done that requires elevated rights requires calling the help desk—and often a lengthy wait.

While Don admits most sales people don't really need elevated rights, he thinks he most certainly does. Without

them he can't install his developer tools, which require regular installation as he updates code, runs tests, and resets everything for the next round.

While perhaps a bit draconian in its implementation, Don's company is well within its rights to heavily restrict administrator rights. Doing so eliminates the possibility that inappropriate software gets onto systems. It also reduces the probability of malware infection, since applications and their configurations are tightly controlled. Maintaining configuration control for regulatory compliance represents yet another valid reason.

Yet his company's rights management means he can't get his job done. His productivity is severely impacted, costing the company untold dollars in wasted time.

Don's desire for administrator rights sounds very similar to the granular approach most IT professionals dream about. That granular approach was first considered way back in 1974 when it was called the "principle of least privilege." While that principle's exact words are unimportant for this conversation, know that least privilege desires to give a person only those

With a little effort and the right tools, you'll find that making the move to granular privilege management has never seemed so easy.

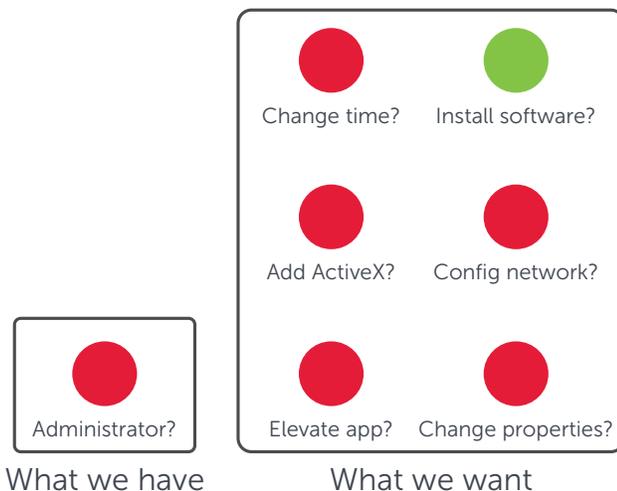


Figure 1. The all-or-nothing rights we have versus the granularity we want

rights that are absolutely essential to accomplishing their assigned tasks.

Implementing the least privilege approach means thinking outside the box of the rights we currently have with Windows today. Figure 1 shows that box in relation to Don's plight. Lacking administrator rights, he's not a productive employee. But at the same time, he doesn't need to perform every action that these rights bring. All he needs is the ability to install software, not necessarily to elevate applications or change system properties.

What he wants—and what least privilege requires—starts by fracturing all the possible actions a person might need to do. Once broken down, that person can be specifically assigned only those actions that meet the requirements of their job. You can't get this out of Windows alone. You need additional tools on both servers and desktops that interact with a centralized management infrastructure to get there.

Problem #2: Getting the necessary granularity

Eloise was just promoted to security officer at her not-quite-small company. Charged with new responsibilities, she immediately aims to eliminate administrator rights all around the network. Doing so, she believes, will overcome many of the daily problems faced by IT. You know the use cases: inappropriate and unlicensed software in places it's not supposed to be, users who break computers by doing things they shouldn't, not to mention IT's inability to control its desktop configuration.

She'll be the star of the company, she thinks, as she ponders that future state.

But beginning the project one day, she quickly finds that pulling those rights isn't as trivial as it seems. Some users actually need them, or at least some portion thereof. Others might not, but their applications do. Removing rights

from the person also removes them from poorly written but necessary applications. When those applications stop functioning, people get unhappy.

To get secure—and earn the promotion she was just handed—Eloise quickly realizes she needs a better approach.

Eliminating administrator rights isn't a project that will happen overnight. Developers need application installations. Users on the road require special consideration. Even the applications themselves are affected when they're not properly coded and require elevation. The steps required to move from "administrator-everywhere" to "administrator-nowhere" are going to take time.

One of the biggest consumers of that time will be figuring out the mapping between users, actions and company policies. These three elements must come together to create the least privilege environment that replaces the death of administrator. Figure 2 shows how those three elements interrelate.

What you require first is a catalog of the possible actions any user might need to accomplish. These are actions like changing the time, installing software, adding ActiveX controls, changing system properties and elevating applications, among others. That catalog represents your master list of actions you'll eventually provision to users. An effective privilege management solution will deliver this catalog via its administrative console.

Your next requirement is a directory of the users who perform the actions you've cataloged. *That directory you already have.* For most of us, the directory our users already authenticate against is Active Directory. If your business has been operating for any period of time, you also have the groups and organizational units that map users to their job roles. Finance users, for example, are in the Finance group, while

Getting the necessary granularity for a least privilege environment requires figuring out the mapping between users, actions and company policies.

Locking down users and applications might seem an easy project at first blush: just pull rights from users and watch the network grow secure. The reality, however, is far from trivial.

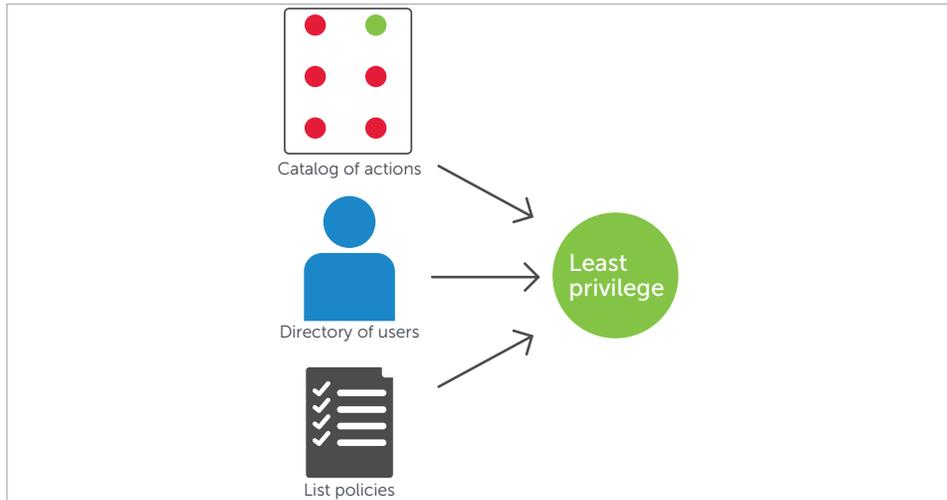


Figure 2. Getting to least privilege requires figuring out the mapping between users, actions and policies.

the sales team occupies the Sales group. You've already been using these groups for assigning rights to files and folders. Now, with a privilege management solution, you're merely extending their use to determine the actions each group will be allowed to accomplish.

The final requirement isn't technical in nature, but procedural. Your business is unique compared to every other business out there, which means that its policies are unique as well. Yet while you probably have a general understanding of those policies, they may not be documented in exactly the same format as your catalog of actions. Gathering your lists of policies and translating them into user actions is the final step in this process.

The integration of these three elements is what defines privilege management that follows least privilege. The granularity gained by their separation is what enables you to balance, for example, Eloise's desire for lockdown with her company's requirement for productivity.

Problem #3: Getting rules that work

Chris manages the sales team at his medium-sized company. He's a great employee with a long track record of performance. Doing his job requires plenty of phone time, and

not a little bit of travel. It also requires a set of applications to which few in the company have access. Those applications report on sales data, and include plenty of sensitive information that would hurt his company if it ever got out.

The problem is that Chris also has another application he likes to use on his company laptop: his file-sharing application, which he keeps around because it brings him music and movies for those long work trips. Having administrative rights for a while, he used them to install that application on his laptop. He's never really considered how "file sharing" and "sensitive data" might not go well together on the same corporate laptop.

The company announced today that they're getting rid of administrator rights. Yet Chris knows both his sales application and his file-sharing application require them to even start up. He needs those rights to do his job. He also hopes he can continue file sharing once they've made the change.

Locking down users and applications might seem an easy project at first blush: just pull rights from users and watch the network grow secure. The reality, however, is far from trivial. Once you begin digging into the instances of



actions you'll assign, you'll quickly find there's a lot of work required before you can see the project finished.

Just installing a privilege management solution doesn't automatically bring least privilege to the network. Any solution is a framework within which rules must be created that map users to policy-approved actions. Chris' situation is fairly common during this period of rule construction: you, the IT professional, want to create a whitelist of only the applications approved for execution and/or elevation. Figure 3 shows one way such a rule might be created.

In the figure, you can see how the application's executable can be referenced by path, file hash or digital certificate. Each has its pros and cons that must be weighed when building the rule. In Chris' case, denying all applications by default and then specifically allowing those that are approved means preserving his sales application while shutting down his file-sharing security hole.

Yet even the smallest business in operation today uses many different applications. A business of ten people might require fifty applications to get

the job done. *Getting the rules that work sometimes requires the assistance of an entire community.*

That's why the privilege management solution you want should include some way to share your rules with others. With a clearinghouse of effective rules, populated by others in similar situations, you can quickly identify the rules that have worked for them. With businesses worldwide looking to eradicate their administrator problem, why reinvent the wheel all by yourself?

Privilege management is the death of the administrator

Evolving your network's security approach to one that follows least privilege is a worthy goal. Getting you there are privilege management solutions that wrap around Microsoft Windows and Active Directory to enable the granularity you've read about here. A solution you'll want starts with a full catalog of actions from which to create rules. That same solution integrates with your Active Directory data to identify users and groups. It also includes collaboration tools that help shorten deployment time and increase rule quality.

Just installing a privilege management solution doesn't automatically bring least privilege to the network.

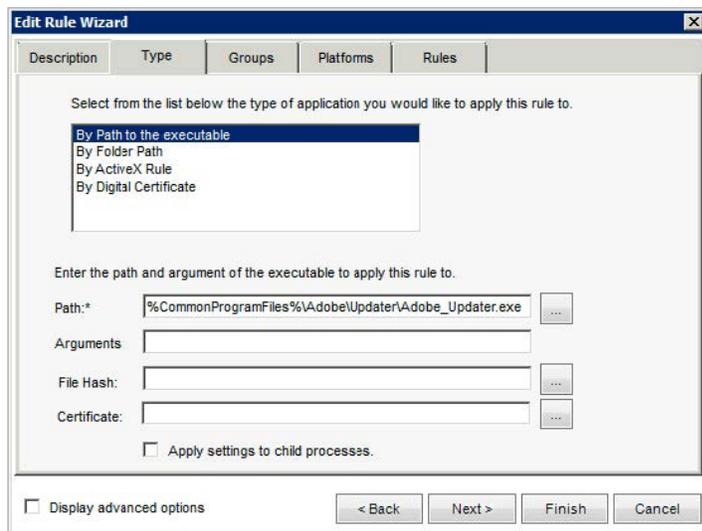


Figure 3. Creating a rule for the execution or elevation of an application.

These solutions exist today.
Implementing them starts by killing
administrator.

About Desktop Authority Management Suite

Desktop Authority Management Suite enables administrators to 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.

With Privilege Manager, you can grant user accounts the least privileges necessary according to best practices, yet elevate specific applications and ActiveX controls as needed. Determine user rights for just those applications, features and controls you choose with the low-cost solution for elevating user rights.

Visit www.quest.com/desktop-authority-management-suite for more information.

About the author

Greg Shields is a senior partner and principal technologist with Concentrated Technology. He is a contributing editor for *TechNet* magazine and *Redmond* magazine, and a series editor for Realtime Publishers. Greg is a sought-after and top-ranked speaker, seen regularly at conferences like TechMentor, Tech Ed, VMworld and more. He is a multiple recipient of Microsoft's "Most Valuable Professional" award and has received VMware's vExpert award.

With Privilege Manager, you can grant user accounts the least privileges necessary according to best practices, yet elevate specific applications and ActiveX controls as needed.



For More Information

© 2013 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.

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

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

