

# The Privilege Management Conspiracy

The Secret War over Elevated User Privilege



## Abstract

There are things you want your users to be able to do—like changing the time zone on their laptops or installing a corporate ActiveX control—that by default require local administrator privileges. You don't really want to incur the security risks of making everyone a local admin, but you can't afford having your help desk keep getting calls every time a user needs to do something that requires elevated privileges. This white paper explores this problem and offers a better way to manage elevated privileges.

## Introduction

There's been a conspiracy in your Windows environment for quite a few years now. A secret war is being waged, and you and your users are innocent bystanders caught in the crossfire.

Here's one example: a software developer creates an application, but in order to get all the bits of the application installed properly, he needs the installer to run under elevated

privileges. This happens so often that you just make your users local administrators on their computers. Now you're opening your company up to security risks from malware that has the potential to affect productivity and expose confidential information.

There are plenty of other scenarios. Your users might want to change the time zone on their client computer, install a corporate ActiveX control, or let their Java virtual machine update itself. Or they just need to run a specific process under elevated permissions, but you're not wild about creating new accounts and passwords for everyone to use for that purpose. So, again, you just make your users local administrators on their computers. But you know you are introducing risks: you want your poor users to be able install Internet Explorer applets like Flash Player, but you don't want them to have full run of all the Internet's ActiveX goodies.

You don't really want to incur the security risks of making everyone a local admin.

Let's face it, despite improvements over the years, there are still things you want your users to be able to do that, by default, require elevated permissions in Windows. So you end up having to choose: force them do without those things, over-privilege your users' accounts, or deal with the additional workload your help desk will incur granting elevated privileges on a case-by-case basis.

There's gotta be a better way.

### **Understanding elevated privileges** **Elevated privileges need to be granular and dynamic.**

The problem is that, whatever you decide to do in terms of elevating users' privilege, it has to be pretty granular. You don't want to have to extend the same elevated permissions to everyone in your environment. Instead, you'll need to identify users by user name, or by organizational unit or group membership, or maybe even by their network subnet or the presence of a registry key or application on their computer.

Your criteria might well be dynamic: if a user has some specific application, then they can get these additional privileges, but you don't want to have to keep a list of who those users are, because who has that application is constantly changing.

You might even want to set up different elevations for different offices and geographic locations, and when a user moves between locations, their ability to elevate privileges should change accordingly.

### **Privilege quiz**

Bob works in a manufacturing plant and frequently runs applications that monitor the operating parameters of the plant's equipment. That software must be run by a local administrator. Bob also surfs the Web and uses email on that computer, and he's well-known for forwarding chain emails and falling for pranks and hoaxes. When Bob visits the company's headquarters, however, he runs only the typical knowledge-worker applications: Word, Outlook and so forth.

How do you make sure Bob can do what he needs?

- A. Just make him a local Admin on the plant computer.
- B. Make him a domain Admin.
- C. Make a separate Admin account for him to use in the plant.
- D. These are all stupid ideas.

### What does “elevated” mean, exactly?

And, by the way, what “privileges” are we talking about, exactly?

Half the time, when someone says “elevated privileges,” it’s a code phrase for “just make them an administrator.” But in fact, “elevated” doesn’t necessarily need to mean “elevated all the way to the maximum possible level.” Permissions and privileges come in a spectrum, and in some cases you may need to elevate the user only a little way along that spectrum, not straight to the heights of administrator-hood.

#### Privilege quiz

Jane has an application that runs pretty well under her normal user account. However, once a month it kicks off a maintenance routine that requires her to have additional operating system privileges. An Administrator has all of those privileges—and many more besides—but Jane isn’t an Admin on her machine.

How do you make sure Jane’s application works?

- A. Just make her a local Admin on the plant computer.
- B. Tell her to just cancel the maintenance routine.
- C. Schedule the maintenance routine to run under Scheduled Tasks using an Admin account.
- D. These are all bad ideas. (Didn’t you get this in our first quiz?)

### When are elevated privileges needed?

Let’s consider the different things that a user might need some privilege elevation for:

- Specific Windows features and processes, like changing the time zone on their computer
- The files in a specific folder, so that a given application can run properly
- Specific ActiveX controls that install into Internet Explorer
- Application installers and updaters
- Approved applications

In short, lots of things. In an ideal world all of this stuff would just work under a user’s normal, lower-privileged account, but in the real world, privilege elevation is a must-have capability.

But you can’t just make everyone a local administrator. Ok, well, you can, but you don’t really want to. Aside from the fact that being administrator gives a user way too much room to create trouble, you just know it’s the wrong thing to do. And organizations dealing with most legislative and industry compliance mandates really can’t make their users administrators.

#### Privilege quiz

Keith travels all over the world for his company. He’s missed more than a few appointments because his PC’s calendar never knows what time zone he’s in.

How do you make sure Keith can update that time zone?

- A. Just make him a local Admin on the computer.
- B. Buy him a World Clock application.
- C. Get him a time zone conversion wallet card.
- D. None of these are really smart. (C’mon, it’s pretty obvious what the answer should be!)

Permissions and privileges come in a spectrum, and in some cases you may need to elevate the user only a little way along that spectrum.

What we need is the ability to give users exactly the right privilege, at the right time, to get the job at hand done.

## Managing elevated privileges

### Lockdown isn't the answer.

We all know that users with too much privilege are liable to do serious damage to their computers and the network. Viruses. Botnets. Spyware. Serious damage. Traditionally, the solution has been just to lock everything down tight as a drum, so that nobody can do anything. The problem is that nobody can do anything, even the stuff they need to do. So a complete lockdown isn't the answer.

What we need instead is privilege management, the ability to give users exactly the right privilege, at the right time, to get the job at hand done. Ideally we'd also want to track those uses of privilege, because that'll help us figure out when a user has messed up their own machine by abusing that privilege.

With managed privilege elevation, you can let users run the higher-privileged things that they need to run—and nothing more. They get to do what they need for their jobs, and you get the security of knowing they're not dropping botnets all over the network using excessive administrator rights. Everyone's happy.

So how do we actually do it?

### Desktop Authority Management Suite delivers the elevated privilege management you need.

Desktop Authority Management Suite from Dell delivers centralized, secure and consistent Windows user environment management, including granular control of privileges. The suite consists of three solutions: Desktop Authority, Privilege Manager and MSI Studio.

Privilege Manager is designed to take the weirdness out of all weird privilege situations discussed above. You can decide exactly what users are able to elevate, and you don't need to give them

an additional user account or password—you don't even need to give their current user account any additional or special permissions. They'll be able to elevate Windows processes and features, install and update applications, and even install and operate ActiveX controls—all under elevated permissions and all under your centralized control.

There's even a free version, Privilege Manager Community Edition, that can help you and your users overcome some of the most annoying limited-privilege scenarios.

Privilege Manager works on a system of rules—you can either make your own rules or copy those created by other administrators through the product's online Rules Exchange. Rules are centrally managed in an intuitive console. A single rule can target:

- Specific applications.
- Specific Windows processes.
- All files in a folder (for when you can't pin down which file is demanding higher privileges).
- Specific ActiveX controls (unlike IE, which either allows or disallows all of them).
- Application installers. You can even have Privilege Manager verify the SHA-1 hash of the installer to make sure it's the one you've approved.
- Files based on their digital signature or publisher's certificate. For example, you could elevate all applications produced and signed by Microsoft.

Once a rule is created, you decide how to apply it to. For example, you can apply it to a collection of given machines, or to specific versions of Windows. Or you can use Privilege Manager's flexible and dynamic Validation Logic, which enables you to deploy rules to specific users, groups, organizational units, computers, groups of computers or IP address ranges, or even to computers having specified registry keys or applications installed. You can get incredibly granular, and the Validation Logic is checked

dynamically, so that users whose situations change have their applied elevation rules also changed.

### Privilege quiz review

How did you do on the quiz?

“D” was the right answer every time, of course—unless you’ve got Privilege Authority. With it, you could have elevated Bob’s plant application and Jane’s maintenance routine, and let Keith adjust his time zone—all without making anybody a local Admin on anything, and without them having to do anything special to run their applications.

Moreover, you can report on all of the activity: whose privileges have been elevated, the frequency of privilege use, the current privilege configuration and more. Get the reports in PDF, HTML or RTF format, or use third-party reporting tools to report directly from Privilege Manager’s SQL Server database.

### Conclusion

In a perfect world, users would never need elevated privilege. But in the real world, they do. With managed elevation, everyone wins: users don’t need to bug the help desk every time they need something serious done, but they’re not able to run rampant with their increased permissions.

Privilege Manager gives you the central control over elevated privilege that you need. Users don’t need to be local Administrators on their computers, but they can still perform the specific actions you permit—even when those specific actions need a bit more privilege than the user normally has.

Check it out. The Community Edition is free, and it will give you a great idea of what Privilege Manager can do. Plus, there are video walkthroughs, edition comparisons and fun cartoons waiting for you at [www.quest.com/desktop-authority-management-suite](http://www.quest.com/desktop-authority-management-suite).

Privilege Manager gives you the central control over elevated privilege that you need.

### 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](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.

