

# Achieving Windows Desktop “Least Privilege” in the Federal Market

By Derek Melber  
Microsoft Group Policy MVP

**November 2010**

## Table of Contents

Overview .....	3
What You Must Know About Administrative Rights .....	3
Compliance Mandates .....	5
US Office of Management and Budgets (OMB) .....	5
US Government Configuration Baseline (USGCB) .....	5
Federal Information Security Management Act (FISMA) .....	6
Information and Communications Enhancement (ICE) Act .....	6
National Institute of Standards and Technology (NIST) .....	6
Challenges to Meet Compliance Mandates .....	7
Powerbroker <sup>®</sup> Desktops Windows Edition Solves all Least Privilege Issues .....	8
Extends your existing Group Policy .....	8
Does not alter domain controllers or the AD schema .....	8
Leverages your Active Directory structure .....	8
Supports all Microsoft supported Windows desktop versions .....	8
Federal Agencies Solve Least Privilege Compliance with PowerBroker <sup>®</sup> Desktops .....	9
US Agencies Using PowerBroker <sup>®</sup> Desktops .....	9
Summary .....	10

## Overview

Some aspects of today's Federal computing world are absolute. First, government and military compliance regulations are severe. Second, these compliance regulations require that all users on every desktop be standard users. This means that desktop and laptop users are not granted administrator rights.

Third, when a desktop user has administrative privileges, disastrous things can, and oftentimes do, occur. There are solutions to these issues, but one solution is more efficient, cheaper, and faster to implement than any. This paper will provide information on what you need to know to make decisions on why, and how to, create secure desktops by implementing the security best practice of "least privilege."

*When an employee is granted local administrative privileges, all control ... not some, not part, not a portion, but all control ... is given to that employee for that desktop.*

### **Definition of the Principle of Least Privilege:**

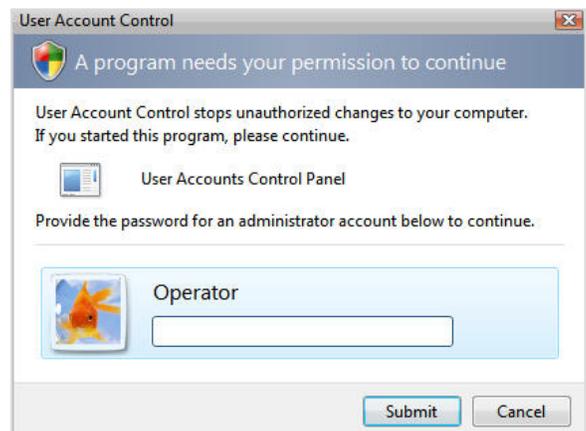
The Department of Defense Trusted Computer System Evaluation Criteria, (DOD-5200.28-STD), also known as the Orange Book, is an accepted standard for computer security. This publication defines least privilege as a principle that *"requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."*

## What You Must Know About Administrative Rights

When an employee is granted local administrative privileges, all control ... not some, not part, not a portion, but all control is given to that employee for that desktop. With that much control, network management is put into jeopardy.

As a local administrator, there are many actions that a user can take that can degrade security, create vulnerabilities, and even generate attacks on the network. To begin with, as local administrator, users can prevent any security policy, established in Active Directory or Group Policy, from becoming effective by simply removing their computer from the domain.

A user does not need to be a domain administrator in order to perform this action. As long as the user is a local administrator for that desktop, the computer can be taken out of the domain. Since the computer is now a stand-alone computer, Active Directory cannot control the desktop, even if it is part of a workgroup.



Another issue is that a local administrator can alter IP address settings. These changes can open up the computer to exploitation, produce loss of access to applications, and even isolate the desktop completely from the entire network. Just a single setting change can have a trickledown effect, causing significant issues and destroying the stability of communication with the desktop.

For example, if the local administrator were to alter the DNS IP address for their desktop so that communication with DNS is lost, then nearly all aspects of Active Directory fail. The only way a desktop can communicate with Active Directory is to first communicate with DNS. If it loses its connection to DNS, then:

- The list of domain controllers will not be obtained
- The KDC (Kerberos Distribution Center) will not be obtained
- Kerberos will not be used as the authentication protocol
- Group Policy will not deploy to the desktop
- Communication with Exchange will most likely fail
- DFS communications will most likely fail
- SharePoint communications will most likely fail
- Authentication might fail
- Access to network resources will become difficult

*Nearly every federal mandate addresses to some degree the topic of local administrative privileges.*

Local administrative rights allow a user to alter settings in the Registry. Actually, every setting that can be altered by a domain admin or Group Policy can be altered by the local administrator. Since the Registry is being altered manually, this will negate the application of Group Policy related Registry settings. Even at the next Group Policy refresh, the manual change to the Registry will remain. There are ways to prevent this behavior. However, default settings made to the Registry, after applying Group Policy, will not be changed at a Group Policy refresh. These settings could involve security, Internet Explorer, applications, the desktop, Control Panel, Registry settings, etc.

Another area of concern is that a user with local administrative privileges can install any application they wish on their desktop. This includes hack tools, virus-ridden applications, vulnerable applications and non-licensed applications. All of the applications cause negative repercussions for the desktop, the network and network management.

For these and other security reasons, enforcement of federal and military compliance mandates have increased with regard to preventing local users from having administrative privileges. It is crystal clear to everyone that when a user is granted local administrative privileges, bad things can, and will, occur.

## Compliance Mandates

Nearly every federal mandate addresses, to some degree, the topic of local administrative privileges. Prevention of these issues, by restricting administrative rights is top of mind for security officials, and the enforcement of these mandates over the last two years have been accompanied by very steep fines. Examples include:

### US Office of Management and Budgets (OMB)

The Office of Management and Budget made it clear to agencies that compliance with the adoption of the US Government Configuration Baseline (USGCB), *previously Federal Desktop Core Configuration (FDCC)*, means all PCs using Windows operating systems must have the standard image. Even though, the OMB expects 100 percent compliance, some realistic and pragmatic issues have to be worked through. Standard Desktop Configuration (SDC) mandates that all government agencies comply with the standard Windows XP, Vista and Windows 7 security configurations.



The mandate affects all government Windows-based desktops that connect to the NIPRNet (unclassified) and SIPRNet (classified) networks. The restriction very clearly states that all local administrative privileges were to be removed by Feb 1, 2008. It also indicates that all tasks are performed with the least privilege and users be logged in with limited user account privileges. It is only administrator-level accounts that need to perform specific maintenance tasks that are to be granted admin level privileges when needed.

### US Government Configuration Baseline (USGCB)

The USGCB defines this mandate and states that all federal organizations employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users), which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

The mandate clearly states that users do not log in to their Windows computers with admin privileges. It also states that no standard user-based changes can be made to standard security configurations.

## Federal Information Security Management Act (FISMA)

FISMA is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. FISMA requirements detailed in section 3544(b) (2) (D) (iii) clearly indicate that all Windows desktop configurations adhere to the following:

- Restricting administration of configurations to only authorized professionals.
- Implementation of the Federal Information Security Management Act of 2002 (Public Law 107-296; 116 Stat. 2135) (A) wastes agency resources on paperwork exercise instead of security; (B) agencies do not fully understand what information they hold, who has access to that information, and whether the information has been compromised.

## Information and Communications Enhancement (ICE) Act

The ICE Act of 2009 is the new FISMA. This is a bill that is meant to amend chapter 35 of title 44, United States Code, in order to recognize the interconnected nature of the Internet and agency networks. The act is designed to improve situational awareness of Government cyberspace, enhance information security of the Federal Government, and unify policies, procedures, and guidelines for securing information systems and national security systems.

Section S.921 calls upon Federal agencies to ensure that they “monitor, detect, analyze, protect, report, and respond against known vulnerabilities, attacks, and exploitations” and “continuously test and evaluate information security controls and techniques to ensure that they are effectively implemented.”

## National Institute of Standards and Technology (NIST)

NIST has been setting standards for government, military and other entities for many years. The NIST 800-53 Critical Control No. 8 sets standards and mandates controlled use of administrative privileges. This NIST mandate clarifies how privileged user accounts should be handled, stating that there be a separation of user privileges. In essence, administrators are defined as users that are authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform. AC-6 (Access Control 6) indicates that least privilege for desktops is a Priority 1 (P1) control and that the organization employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

## Challenges to Meet Compliance Mandates

Almost every company, corporation, or government agency has at one time or another come upon a situation on a desktop where maintaining least privilege become an issue.

The issue may not be complicated, but solving them while maintaining compliance with federal mandates has become an issue. Here are a few situations where desktop users are allowed to run as local administrators, even if temporarily, in order to lessen the impact on resources:



- **Installation of applications or drivers**

The installation of applications packaged as executables and MSIs often requires administrative privileges in order for the installation to complete. This is because application installations often require access to a protected file, folder or Registry key.

- **Installation of a driver**

Installing drivers for a new USB device, removable storage device, video/audio device, printer, and other devices typically requires the installer to have local administrative privileges. Like application installation, this is required to allow access to a protected file, folder or Registry key.

- **Installation of ActiveX Controls**

Organizations are considering moving functional areas (HR, Financials and Inventory) to cloud computing. This requires access via the Internet with its increasing use of ActiveX controls to manage access. The installation of ActiveX controls requires that the user performing the installation have local administrator privilege.

- **Perform routine operating system functions**

Although Windows 7 has been altered to allow some routine operating system functions to be performed by a standard user, there are still some functions that require local administrative privileges. For Windows XP, the list is rather long, including installing local printers, changing the time zone, defragging the hard drive, etc. Regardless, these actions are encouraged and should be allowed by the local user; however, they should be running as a standard user instead of a local administrator.

- **Run third-party and in-house applications**

The list of applications that require local administrative privileges can be overwhelming for a department, agency, company or any entity for that matter. It does not matter if the application was purchased by a major vendor, small vendor or built in-house. Many applications require the user to be a local administrator in order to run fully.

## **Powerbroker® Desktops Windows Edition Solves all Least Privilege Issues**

The BeyondTrust solution to the Least Privilege issue for desktops is PowerBroker® Desktops. This simple, efficient, non-obtrusive solution provides compelling benefits:

### **Extends your existing Group Policy**

If you are running Active Directory, you have all you need to implement PowerBroker® Desktops. Group Policy is built into Active Directory and into every desktop that can be a part of an Active Directory domain. Windows 2000, XP, Vista and Windows 7 desktops all support Group Policy from Active Directory just by joining the domain. Since you have Active Directory and run these desktop operating systems, you just simply need to extend Group Policy to implement PowerBroker® Desktops.

### **Does not alter domain controllers or the AD schema**

Since Active Directory supports Group Policy by default, extending Group Policy does not require any alterations to the AD schema. The AD schema already has every setting needed to support any extension to Group Policy. Domain controllers do not need to be altered in anyway, and it is a best practice to not install anything regarding PowerBroker® Desktops on any domain controller unless you want to achieve least privilege for your IT staff, in addition to typical employees.

### **Leverages your Active Directory structure**

Most organizations have designed Active Directory to support their existing Group Policy. Since Active Directory has been designed to control desktops and servers, it is ready to support PowerBroker® Desktops. This means that you can implement PowerBroker® Desktops to only a portion of your employees during your pilot and then implement it to all users after the pilot is completed.

### **Supports all Microsoft supported Windows desktop versions**

The majority of organizations today run Windows XP and Windows 7. However, there are still some Windows 2000 desktops and Vista desktops. The advent of 64-bit desktops has also revolutionized and made desktop computing more efficient. PowerBroker® Desktops support all of these operating systems, including all versions of 64-bit Windows desktops.

## Federal Agencies Solve Least Privilege Compliance with PowerBroker® Desktops

Here is how PowerBroker® Desktops helped Mike De Bruin of the US Air Force:

*PowerBroker® Desktops has helped us to meet Air Force standard configuration requirements more efficiently and eliminate end-user administrative privileges, while decreasing the need for IT support.*

*PowerBroker® Desktops enables our end users to continue using numerous applications that require administrative privileges and perform necessary system tasks such as adding a local printer or defragging the hard drive while still meeting the government mandate. As other government agencies seek to comply with the OMB requirements, their efforts will be made considerably easier by adopting BeyondTrust PowerBroker® Desktops.*

Mike DeBruin

Senior Systems Engineer, Vandenberg Air Force Base

<http://www.beyondtrust.com/company/pressreleases/21May2007.aspx>

## US Agencies Using PowerBroker® Desktops

It does not matter how many desktops your organization supports. They can all be placed into least privilege mode by implementing PowerBroker® Desktops. Any size agency or section of an organization can leverage PowerBroker® Desktops to implement a least privilege environment. This is a small sample list of some Federal organizations that have already implemented a least privilege environment using PowerBroker® Desktops:

- Department of Agriculture
- Department of Defense
- Air Force
- Army
- Navy
- Census Bureau
- Postal Service
- Department of Veterans Affairs
- Department of the Treasury
- Department of Labor
- Department of Commerce
- Department of Energy
- Government Accountability Office
- Office of Comptroller of the Currency
- Department of Transportation
- US Environmental Protection Agency
- Federal Deposit Insurance Corporation

## Summary

PowerBroker® Desktops solves “least privilege” for organizations by allowing employees to run as standard users, while performing authorized tasks and actions. Organizations who grant local administrative privileges to users in order to perform tasks and actions, can benefit in reduced malware and exploits, while improving productivity, by implementing PowerBroker® Desktops.

PowerBroker® Desktops allows standard users to run authorized tasks and applications, including installing applications, device drivers and ActiveX controls, as well as performing routine operating system tasks. It does not require a backend server or alterations to the existing Active Directory schema. It does not require installation on a domain controller, nor alterations to Active Directory for implementation. PowerBroker® Desktops can be quickly implemented solving your least privilege dilemma within a short time period.