Realtime publishers

The Essentials Series:
Fulfilling Compliance by Eliminating Administrator Rights

Fulfilling FDCC Compliance by Eliminating Administrator Rights

sponsored by

beyondtrust®

by Greg Shields

Copyright Statement

Fulfilling FDCC Compliance by Eliminating Administrator Rights

There's a problem with the widespread distribution of administrator rights in your organization, and it has nothing to do with security.

That problem is compliance: Compliance with the industry, governmental, and regulatory statutes that define certain configurations within your IT infrastructure. Although many of those configurations are mandated to enforce a greater level of security control, your job as IT professional is to ensure their fulfillment.

However, similar to the tradeoffs we endure between strong security and total usability, the solid implementation of a compliant configuration often requires a reduction in user flexibility, administrative capability, and merely getting the job of IT done. Nowhere is this more prevalent than in compliance's role in reducing the power and spread of administrative rights.

Understanding the FDCC

In the spaces bound by the federal government as well as its contractors and partners, new rules have been drafted that dramatically change how federal desktop configurations are locked down. Falling under the Federal Desktop Core Configuration (FDCC), these rules mandate hundreds of very specific configurations that must be enabled on any desktop that connects to a federal network.

The FDCC is a security configuration that began with a 2007 memorandum by the United States Office of Management and Budget (OMB). That memo discusses the need for a centralization of effort in defining a central configuration for all desktops contained within federal IT environments. Such a unified configuration would strengthen federal IT security by mandating a tested configuration across all federal IT organizations.

This configuration would additionally provide a standardized starting point for external vendors, easing their process with developing solutions that work across the whole of government IT. In conjunction with the FDCC, the OMB also began work on the Security Content Automation Protocol (SCAP), a cross-platform vulnerability management protocol that enables outside vendors to validate their products' functionality with FDCC desktops as well as other regulations required by government systems.

For Microsoft operating systems (OSs), today's FDCC provides guidance for the Windows XP and Windows Vista OSs, describing a list of registry changes and Group Policy changes that must be implemented across all desktops. These changes span from disabling unnecessary services and applications to configuring firewall rules to adjusting user account and event log settings. Currently a version 1.0 release, the specific guidance can be downloaded from the Web site of the National Institute of Standards and Technology (NIST) at http://nvd.nist.gov/fdcc/index.cfm.

You'll find that the FDCC's guidance is exceptionally specific. In comparison with other compliance regulations usually associated with private industry—and highlighted in the other papers of this Essentials Series—the FDCC's guidance is generally considered the most specific. Unlike other regulations, the FDCC documents the exact settings within the Windows OS that must be set to be considered compliant.

FDCC, Admin Rights, and the Goal of Least Privilege

Implementing the FDCC's configuration dramatically changes the user's operating environment in a number of very key ways. One of those is in the elimination of administrator rights as a primary logon for users. Individuals who require administrative privileges for the administration of the IT environment will be assigned a secondary logon that must be used only for accomplishing activities that require its level of privileges. This access is granted by waiver only. Effectively, the FDCC eliminates administrative privileges for all but the very few who are members of IT.

Although this change in protocol will have the positive effect of increasing the level of overall security, at the same time it stands to reduce the agility of users. These users are those whose job role requires them to regularly switch between administrative and non-administrative functions throughout the day. According to the FDCC's guidance, users are directed to log out of this account and log back in with their standard user account once their administrative action has completed.

Of greater significance is the effect that the FDCC will have on typical users who are not IT administrators. These users will no longer be permitted to log in as an administrator and may only have a standard user account. This setup will not only increase security but also ensure that users cannot alter the defined standard desktop settings. With administrator rights, a user may configure his or her computer as they see fit. However, the OMB's mandate to comply will impact the functionality of certain software packages that require administrative privileges to function. Some software packages simply will not work without administrative privileges. Whether through poor coding or architecture, a legacy approach to permissions, or other fallacies on the part of the software, use of this software requires the user to have administrative privileges. As such, a strict adherence to the FDCC guidelines can prevent some software from successfully running on federal computers.

Although not explicitly stated, it is generally accepted that a central goal of FDCC as well as every other industry, governmental, and regulatory compliance statute is the implementation of Least Privilege. The Principle of Least Privilege was developed more than 30 years ago by the United States Department of Defense (DoD). This principle "requires that each subject in a system be granted the most restrictive set of privileges…needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."

By eliminating administrator privileges from your environment, you are moving that environment towards one that fulfills this principle's goals. You are at the same time going far towards fulfilling the requirements of regulations such as FDCC.

Yet Least Privilege is more than simply eliminating administrator rights. Least Privilege can more broadly be described as the intersection of the user's role in the organization, the overarching corporate security policy of that organization, and the tasks that are available to be accomplished within the IT infrastructure. In effect, an environment that fulfills the requirements of Least Privilege will be very granularly capable of providing access to each person based on their needs.

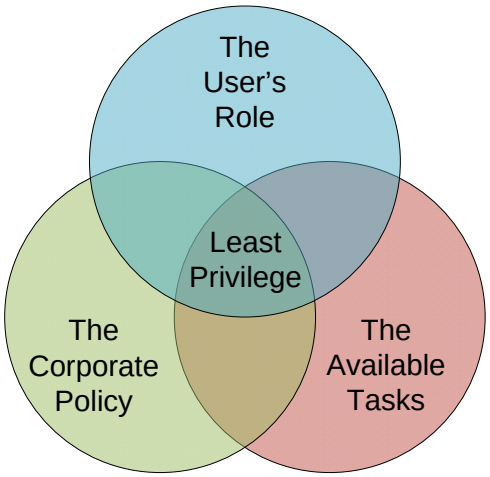

Figure 1: Least Privilege's elimination of administrator rights is really the combination of three factors.

For a comprehensive look at Least Principle's three overlapping requirements as well as how the effective elimination of administrator rights requires the involvement of each, check out *Essentials Series: Eliminating Administrator Rights*, found at http://www.beyondtrust.com/wp_ElimAdminRights_download.aspx?source=Realtime.

Unfortunately, the Microsoft Windows OS alone does not natively provide the architecture to enable this granular control. Using the Microsoft Windows OS, it is possible to eliminate the privileges assigned to an individual. However, these person-based privileges are far too coarse in their application. For example, with poorly-coded applications, simply removing administrator rights from a user may actually prevent needed applications from functioning. Other system configuration changes, like connecting to a local printer, can also require administrative rights, making their removal a problem for the user.

Summary

Organizations that fall under the scope of FDCC should consider the use of external solutions that extend the granularity of privileges assigned. Such tools enable privileges to be assigned to applications based on user roles, adding that necessary granularity while still fulfilling the requirements of governmental mandates. These tools also provide the right level of audit-friendly logging that tracks user and administrator actions across systems, ensuring you meet your compliance regulations' requirements for activity tracking.