

Building a Secure and Compliant Windows Desktop

White Paper

Improving desktop security is a priority for nearly all companies. This is fueled by an increased recognition of the threat unsecured desktops pose, as well as a need to meet compliance regulations. However, most companies have struggled with implementing new security solutions. Removing administrator rights from end users when they log into their desktop is the Holy Grail of desktop security.

Implementation of this level of security has been difficult due to the fact that ordinary activities an end user needs to do for their job, such as running certain applications, performing authorized installations, or managing certain desktop settings require users to have administrative privileges. This "LUA bug" has plagued corporate America since the onset of PCs on every desk.

The good news is that the technologies exist to eliminate the need for end users to have administrative privileges on their desktop to perform their job tasks. This paper presents the benefits of removing administrator rights from end users, the combination of technologies needed for effective implementation of this level of security, and how to best remove the local Administrator account, while maintaining the users' access to all applications.

Document Revision 1.00

Author
Derek Melber, Microsoft MVP, MCSE, CISM

About the Author

Derek Melber is a Microsoft Certified Systems Engineer (MCSE), a Microsoft MVP (Windows Server – Group Policy), and a Certified Information Security Manager (CISM). Derek provides consulting and training for many of the Fortune 500 companies on AD, security, and Group Policy. He has written over 15 books and eBooks over the past 5 years, including the only book that Microsoft has ever produced on Group Policy, *The Group Policy Guide*, the soon to release *Group Policy Resource Kit* by MSPress, and the only books available on auditing Windows security, published by The Institute of Internal Auditors. You can reach Derek at derekm@braincore.net.

© 2007 BrainCore.Net AZ, Inc.

Contents

- Introduction** 4
- Principle of Least Privilege** 4
- Benefits for Implementing LUA** 5
 - Increased security 5
 - Increased manageability 5
 - Increased productivity 5
 - Reduced costs 6
 - Reduced piracy and legal liability issues 6
 - Compliance with Mandates 6
 - Increased Data Protection 7
- Limitations of LUA** 7
- Default and Controllable Security Options for Desktops** 7
 - Local Group Membership 8
 - Group Policy Security and Software Controls 9
 - User Account Control 10
- Implementing Least Privilege** 11
 - LUA Step 1 – Removing Users from Local Administrators Group 11
 - LUA Step 2 – Resetting the Local Administrator Password 11
 - LUA Step 3 – Configure Applications that Users Can Run Elevated 12
 - Combining LUA with UAC 12
- Summary** 13

Introduction

The implementation of the Principle of Least Privilege and Least Privilege User Access (LUA) are solutions to users requiring administrative privileges on their desktop.

Everyone knows the story about corporate desktop security. If you ask 100 different companies about their end user desktop security, you will find that over half don't have any security beyond the ubiquitous and all too ineffective firewall and antivirus software. While three-quarters of the companies are actively trying to improve their desktop security, they feel as if they don't have a viable solution. This is how it has been for a longtime in corporate America.

Unfortunately, it is still the same story in corporate America today. For many people searching for a security solution it is like trying to read a mystery novel for the 10th time, all the while hoping to find a different ending. Unfortunately, the story of corporate users using their desktop computer as Administrator has not changed, just as your novel will not write a new ending on its own.

The implementation of the Principle of Least Privilege and Least Privilege User Access (LUA) are solutions to users requiring administrative privileges on their desktop. The "LUA bug" is defined as the set of ordinary activities a user has to do in their course of business, such as running applications, performing authorized installations, or managing certain desktop settings that require users to have administrative privileges. This "LUA bug" has plagued corporate America since the onset of PCs on every desk. The good news is that there are solutions and LUA can be achieved, allowing corporations to greatly improve corporate desktop security. There are reasonably priced and efficient methods to provide a way for standard employees to use their desktop with "least privileges" and remove their need to run as Administrator. Using existing Microsoft technologies, combined with some third party solutions, the "LUA bug" can be exterminated and the ending to the story of corporate desktop security rewritten.

Principle of Least Privilege

The term Principle of Least Privilege has been thrown around for many years, many times over, and in many venues. It was defined best by the United States Department of Defense. The Department of Defense knows very well the ramifications of allowing users to run with excess privileges, as well as the benefits of having a user to run with limited privileges on their desktop. The Department of Defense defines the Principle of Least Privilege as:

"[The Principle of Least Privilege] 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." ⁱ

Benefits for Implementing LUA

If you are not firsthand experiencing the issues related to a user having administrative privileges on their desktop, I am certain you can see the potential negative impact that it can have for a company. The benefits of achieving LUA on each and every desktop in a corporate environment are compelling. Every company that I have spoken with wants to achieve LUA, and mainly for the following benefits.

Increased security

If you have granted a user to be Administrator on their desktop, you have relinquished all control over that desktop.

You must consider the security ramifications of a desktop where a user has administrative privileges. In this environment, the user can do anything to the desktop, at anytime. This includes installing new applications, modifying security settings for the desktop, accessing and running every application from the Internet. In essence, if you have granted a user to be Administrator on their desktop, you have relinquished all control over that desktop. Therefore, if you can eliminate the user from running with administrative privileges, you will increase the security of that desktop by stopping the user from installing and running any application they desire. Even more important is that removing administrative privileges will reduce malware. If a user can't install software, then there is little chance that a virus or other malicious software will be introduced by installation.

Increased manageability

When LUA is obtained and users are no longer Administrator on their desktop, it provides an environment where the network administrators can do their job more efficiently. It creates a clear boundary on the desktop. The boundary separates what the user should and should not do, allowing the network administrators to solely make the desktop management decisions. If users can alter the settings made by network administrators, it provides an unmanaged environment that is extremely unstable and unpredictable. LUA eliminates this by removing the users' destructive capabilities.

Increased productivity

The requirements and time that it takes to reinstall a user's desktop is very high. There are so many applications, settings, configurations, and environment complexities that come with installing an end user's desktop. When the user has the ability to install and run any application they desire, these settings easily get altered. In most cases, the applications that are required for the company to run will break or malfunction. The ability to install and run any application also invites spyware, malware, viruses, and other malicious software that is dedicated to breaking the desktop. The continued stability of a desktop that is running with LUA will increase the productivity of the end user, as well as the IT staff.

Reduced costs

Time is money. The time that a user spends waiting for their computer to be “fixed” after a malicious attack due to a non-approved installed piece of software is eliminated with LUA. By prohibiting users to install unauthorized software there is little chance for a virus or other malicious software to install. If the user does not have administrative privileges, the malicious applications on the Internet are powerless, because they won’t be able to access the key areas of the computer as a limited user which is defined by LUA. With all of these reductions in downtime, users and IT staff alone will be able to spend more time on their job, reducing the cost associated with users running with administrative privileges.

Reduced piracy and legal liability issues

Although we all want to trust our users in a corporate environment, there are bound to be a few exceptions to our trust. If you are granting users administrative privilege over their desktop, you are in essence granting them the ability to pirate software and potentially create a legal liability issues for the corporation. For a company and IT staff to turn their head and allow such behavior does not diminish the fact that it is happening. Thus, it does not exonerate the company from the consequences that come along with the prosecution that will come from the behavior. However, if LUA is implemented, these issues are no longer a consideration, as the user will no longer be able to install non-approved software.

Compliance with Mandates

According to the new U.S. federal government regulations... it is no longer acceptable to have users running with administrative privileges.

One of the most compelling reasons for implementing LUA is to meet security compliance requirements. According to the new U.S. federal government regulations, that are going to be mandatory in February 2008, it is no longer acceptable to have users running with administrative privileges. In the memorandum dated March 2007, from Karen Evans, Administrator for the Office of E-Government and Information Technology, she details exactly what the requirements are to meet the new Federal Information Security Management Act (FISMA). The new FISMA requirements detailed in section 3544(b)(2)(D)(iii) clearly indicates that all Windows XP and Vista configurations the following must be adhered to:

“Restricting administration of these configurations to only authorized professionals.”ⁱⁱ

The new regulations clearly state that all federal agencies must comply with standardized Windows XP and Windows Vista security requirements.ⁱⁱⁱ The most important of these requirements as stated by the Office of Management and Budget is that agencies must restrict administrator rights on all desktop computers.^{iv}

Sarbanes-Oxley, Graham-Leach, ITIL, HIPAA, COSO, FERPA, etc. provide general security guidelines and recommendations regarding desktop security. Within each is the clear intention to have users running with least privilege. Ask any security auditor, including myself, how they interpret the

regulations and they will be very quick to state that all users should be running as a non-Administrator with least privileges.

Increased Data Protection

Another important reason that you should implement least privilege is to protect key data for your company. Of course this goes beyond just restricting desktop access, but it is an essential piece. If users are allowed to install any application and run any application from their desktop, it opens up a lot of “attacker” and “hacker” programs that would otherwise be negated if the user was running with least privileges.

Limitations of LUA

All of these reasons, plus any other reason you can drum up, have limitations. The limitations make it very difficult to restrict the user to running with least privileges on their desktop. The limitations are numerous, but these are the top limitations that prohibit or impede companies from implementing least privilege access for users.

- Applications that require the user to have administrative privileges or have membership in the Administrators group
- Access to key Web sites that run applets, Java scripts and ActiveX Controls that require administrative privileges
- System settings such as installing a local printer, defragging the hard-drive or installing hardware that require administrative privileges and make the user productive for their job
- Authorized unmanaged software installations that require administrative privileges

All of these limiting factors require that a user have administrative privilege to their desktop, or some other technology must be in place. There are technologies that solve these limitations, but there is no silver bullet for solving the very complex issues around users running with least privilege. However, with the right combination of technologies that exist today, LUA can be achieved efficiently and in a cost effective manner.

Default and Controllable Security Options for Desktops

Breaking down the key aspects of running with least privilege exposes the true nature of the problem. The problem stems from the fact that applications and installations must be performed as a user with administrative privileges. This core issue has brought to life some different solutions for trying to fix the issue. When evaluating these solutions for a current Windows desktop, you must first evaluate the default security

settings, in conjunction with ways to control the different aspects of the solutions.

If you break down the security options for desktops, you will find that there are some key settings that can be controlled to help with the issues. The question is whether or not these settings solve the problem, or if there are other issues that still need to be resolved. The settings can be broken down into three different areas:

- Local Group Membership
- Group Policy Security and Software Controls
- User Account Control

These three areas are important as they all three tie directly into the issue of a user running with least privilege. It is not only important to see where these areas succeed and fail, but to delineate the differences between default settings with those that are established by normal business practices.

Local Group Membership

The mechanism that is used to elevate a user to have administrative privileges is to add them to the local Administrators group on the desktop. There are additional groups, such as Power Users, on a desktop, but the Administrators group is the only group that has enough privilege to solve all issues for running applications. It is also worth noting that an educated user will find it easy to elevate their privileges from the Power Users group to Administrators. This is why Microsoft has removed the Power Users group Windows Vista and I do not recommend their use in corporations.

The default settings for the local Administrators group are secure. The only user that has membership in this group initially is the local Administrator account. When the computer is joined to a Windows Active Directory domain, the Domain Admins group from Active Directory is automatically placed in this group as a member. Note a few things about the default Administrators group and administrative privilege for the user:

1. There are no user accounts from the domain having membership in the Administrators group by default
2. The only ways a user can obtain elevated privilege on their desktop by default is to be added to the Domain Admins group or to be added to the local Administrators group

This clearly means that the as far as group membership goes, a default installation of a Windows desktop is secure. Least privilege is not a Windows issue! Least privilege is an application and management issue that affects Windows computers.

Group Policy Security and Software Controls

Windows XP and Vista have a tremendous amount of Group Policy settings (a Windows Vista desktop contains over 2000 settings alone). These settings range from security, to Internet Explorer controls, to printer mapping, and more. In addition, Group Policy includes a feature called Software Restriction, which allows administrators the ability to control which applications are able to run on a desktop.

There are some default security settings established from Group Policy. Group Policy establishes the following security settings in a fresh installation of Active Directory:

- Password Policy
- Account Lockout Policy
- Force logoff when logon hours expire
- Encrypting File System is Enabled
- Administrator from domain is the Data Recovery Agent for EFS

By default there are no Software restriction controls established using Group Policy. This means that any application can be installed and run, as long as the user has the correct privileges based on the application requirements.

Software controls via Group Policy are not required, unless you give the user administrative privileges. However, if you provide administrative privileges to the user, software controls are only partially functional. Software controls using Group Policy can't block the installation of an application, nor the running of some applications.

The use of Group Policy settings to control least privilege has been successful for some, but the time and effort is painstaking, and it does create new security concerns. The best configurations in a Group Policy Object (GPO) to control applications include the File Permissions and Registry Permissions. These two areas in a GPO allow the administrator to set the Access Control List (ACL), which provides access to the files, folders, and Registry keys on the target computer. This has been successful in some instances where the applications that require administrative privilege can be given the correct access by adding the user account to the ACL. The user is still logging in as a limited access user, but is granted explicit access to the resources necessary to run the application via the permissions set through Group Policy.

The limitations of this solution are that there are hundreds of applications in a corporation that require this detailed attention. The time to determine each file, folder and Registry key can take hours or days per application. If the application changes version or has an update, it could require more attention for setting permissions. An even greater drawback of this approach is the security risk. All of the files, folders, and Registry keys which you have made

available, in order to allow a single application to run, are now accessible to all applications, including all sorts of malware.

User Account Control

“The combination of elevating approved applications transparently with Privilege Manager and running UAC in no prompt mode with Internet Explorer in protected mode provides a best-of-breed solution to the least privilege problem.”

User Account Control (UAC) is an excellent technology for what it provides to the desktop. UAC is designed to help with the LUA bug and is highly successful at accomplishing this for administrators. However, for the standard end user, UAC does have limitations for what it solves.

By default, UAC is enabled and will prompt the end user for administrative credentials when a program or task that requires such credentials is accessed. It is here that UAC does not meet the overall goals of least privilege. To work with these parameters, the administrator password would need to be provided to users (thus destroying least privilege completely) or an administrator would need to input credentials every time that a user needed to run an application or task requiring such elevated permission. According to Mark Russinovich, a Microsoft Fellow, the over the shoulder solution is not recommended for enterprises. He states in a recent TechNet Magazine article,

"Even though elevation dialogs appear on a separate secure desktop, users have no way by default of verifying that they are viewing a legitimate dialog and not one presented by malware. That isn't an issue for [administrator account mode] because malware can't gain administrative rights with a faked Consent dialog, but malware could wait for a standard user's OTS elevation, intercept it, and use a Trojan horse dialog to capture administrator credentials. With those credentials they can gain access to the administrator's account and infect it. For this reason, OTS elevations are strongly discouraged in corporate environments." ^v

You should not throw out the baby with the bath water here though. As an alternative to prompting the user for over the shoulder administrative support, you set UAC to silently fail to run the application. Although this is only part of the solution, Microsoft's Windows Client Security Product Management Director, Austin Wilson, says that following about combining UAC with other technologies,

"Microsoft recognizes that to help create a secure, auditable and compliant enterprise environment all users should be Standard Users and ideally not have administrative privileges or access to administrator passwords. BeyondTrust Privilege Manager helps corporations that need to allow standard users to run applications that require administrative privileges on Windows Vista with UAC enabled without any prompts or input required from the user. I am pleased to see third-party security vendors such as BeyondTrust improve what is already our most secure business client OS, Windows Vista,... The combination of elevating approved applications transparently with Privilege Manager and running UAC in no prompt mode with Internet Explorer in protected mode provides a best-of-breed solution to the least privilege problem." ^{vi}

UAC is required for desktops to help protect against malware, viruses, adware, and other malicious applications that can be run locally, from the Internet, or even within poorly designed and created applications. The goal is to have UAC protect against the applications that do require administrative privilege, yet are not approved to run. This combination with a solution that does allow a user to run with least privilege and still run applications that require administrative privileges is an ideal solution.

Implementing Least Privilege

The LUA bug is not an easy solution to achieve, or is it? Most companies try to only use a single vendor or technology suite to solve the LUA bug. This approach is difficult to achieve, because there is no such solution available. Achieving LUA on the desktop is a solution that requires many different technologies combined together. The great thing is that most of them are available free from Microsoft. They include new technologies or technologies that you never thought could be used in conjunction with others to solve the LUA bug. Below I have detailed out what technologies you need to combine. Solving the LUA bug is a three step process.

LUA Step 1 – Removing Users from Local Administrators Group

The only way a user can have administrative power over their desktop is to be included in the local Administrators group on their computer. This must be cleaned up, as it will immediately remove the user from having any administrative capabilities on their desktop.

This can be a very time consuming process. Consider removing a single user account or group account from every desktop in your environment. That could take months, or even years, depending on how many desktops you have and the location of the desktops.

There is a better solution, which is to use Group Policy. Windows Vista and Server 2008 will provide a solution that you can modify the local Administrators membership, without destroying the integrity of the other members. The solution is new, as it was acquired in 2006 from a company named DesktopStandard. As the solution is Group Policy based it is easy to configure and apply policy. Within just a few hours, the user accounts and group accounts that you specify to be removed will be automatically removed.

(Note: If you have Windows 2000 or pre-Windows XP SP2 desktops, you can still obtain this technology from DesktopStandard to control those desktops.)

LUA Step 2 – Resetting the Local Administrator Password

If the user of the desktop has had any administrative capabilities, chances are very good that the user modified the local Administrator account password to a value they are aware of. If you proceed with Step 1, but don't alter the Administrator password, the user can still logon with the local Administrator account to have elevated privileges. Therefore, you must reset the local Administrator account password.

Like Step 1, if you consider altering this password for every desktop in your environment, it will take you too long before you can ensure that your Step 1 setting is not altered by the local Administrator account.

Again as in Step 1, Group Policy can also solve this issue. Group Policy with Windows Vista and Server 2008 will also include a new policy that allows you to reset the password for any local account, including the Administrator account. Since it is Group Policy based, you can have a consistent password for all desktops, or organize your passwords per department, employee type, location, etc. combine this setting with the Step 1 setting and you can achieve these two steps in just a few hours for every desktop in the company.

(Note: If you have Windows 2000 or pre-Windows XP SP2 desktops, you can still obtain this technology from DesktopStandard to control those desktops.)

LUA Step 3 – Configure Applications that Users Can Run Elevated

The final step is to use a solution like BeyondTrust Privilege Manager to elevate the appropriate applications that require users to have administrative privilege. This step is essential, as it does not alter the logon credentials of the user. The user still logs in with a single set of credentials, all the time functioning as a limited user.

Privilege Manager is then configured in a Group Policy to include all of the applications that a user will need to run, which require administrative privilege. Privilege Manager, on the fly, injects the Administrators group SID into the users process token for the application, granting them dynamic, administrative access to the application. The user only has administrative access to this single process and continues to have limited user access to all other tasks, applications, and functionality on the computer.

This solution is seamless to the user, as there are no prompts, warnings, or interaction required. The application just runs! When the application is closed, the token for that process is deleted, thus eliminating any administrative access for the user account until that application (or another approved application) is launched.

Combining LUA with UAC

Now that LUA is implemented, the rest of the computer must also be protected. Privilege Manager does not provide additional protection above what is gained from removing administrative privileges. This is where UAC comes into the picture. UAC allows Internet Explorer to run in protected mode, providing additional protection to the user from malware, malicious applications, Trojans, or worms when running Internet Explorer. As stated above by Austin Wilson from Microsoft, using UAC in no-prompt mode with BeyondTrust Privilege Manager is an ideal solution. This solution combination provides everything that is needed to control the user environment. The user is running with limited privileges at all times. The application process only runs with administrative privileges when administrative privilege is required and when the application is completed, the limited scope of elevated privilege is removed.

Summary

Desktop security has become a key factor for every company. There is not one company in existence that would not jump at the chance to have end users running with limited privileges, while still maintaining use of all of their required tasks and applications. As long as a company is making money and productive end users should have limited privileges.

The LUA bug is not a Microsoft issue. However, it affects nearly every single desktop that runs Microsoft Windows software. The LUA bug is a development and application issue. Since the developers and application vendors continue to ignore security procedures during the creation of their products, the LUA bug must be handled in other ways.

Using the multi-step approach of combining technologies, LUA can be achieved on every Windows desktop. The modification of the local Administrators group members, altering the local Administrator account password, and giving users access to all applications as a limited user solves the LUA bug. All of these technologies exist and are easily implemented. Their combination will not only protect a desktop from the majority of malware, adware, and malicious programs that are constantly attempting to attack it, but also from the user who knowingly or unknowingly can damage the desktop.

Citations

- ⁱ Department of Defense, Trusted computer system Evaluation Criteria, (DOD-5200.28-STD), or the orange book
- ⁱⁱ Karen Evans, Administrator Office of E-Government and Information Technology, MEMORANDUM FOR CHIEF INFORMATION OFFICERS, http://cio.gov/documents/Windows_Common_Security_Configurations.doc
- ⁱⁱⁱ Microsoft, Windows Vista Security Guide (Used as basis for OMB compliance), <https://www.microsoft.com/technet/windowsvista/security/guide.aspx>
- ^{iv} Government Computer News, Vandenberg Air Force Base delivers user privileges within configuration requirements, http://www.gcn.com/print/26_12/44351-1.html
- ^v TechNet Magazine, Inside Windows Vista User Account Control, <http://www.microsoft.com/technet/technetmag/issues/2007/06/UAC/default.aspx>
- ^{vi} eWeek, BeyondTrust Reins in Vista UAC Prompts, <http://www.eweek.com/article2/0.1759.2173877.00.asp?kc=EWRSS03119TX1K0000594>

Legal Disclaimer

This document is for informational purposes only. Microsoft, Microsoft Group Policy, Microsoft Internet Explorer, Microsoft Windows, Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista and DesktopStandard are trademarks of Microsoft Corporation. BeyondTrust and Privilege Manager are trademarks of BeyondTrust Corporation. Other names mentioned herein may be trademarks of their respective owners.