Principles of Least Privilege

Privilege creep

Privilege creep is the gradual accumulation of access rights beyond what an individual needs to do his or her job. In information technology, a privilege is an identified right that a particular end user has to a particular system resource, such as a file folder, system, or machine.

Privilege creep often occurs when an employee changes job responsibilities within the organization and is granted new privileges. While an employee may need to retain his or her former privileges during a period of transition, those privileges are rarely revoked and result in an unnecessary accumulation of access privileges.

Privilege creep, which is a common problem in IT organizations of all sizes, creates a two-fold security risk. First, an employee with excess privileges may be tempted to use those privileges inappropriately. Second, if an intruder gains access to an end user's account -- and that end user has excess privileges -- the intruder will also have excess privileges. Either scenario poses a risk that could result in data loss or theft.

Least Privilege Best Practices

Organizations that want to (or must) implement least privilege can begin by following these best practices:

- **Adopt "least privilege as default."** This principle is so fundamental it should be the default mind-set for all security professionals yet, surprisingly, many organizations do not adequately enforce it. One data risk study of nearly 800 companies found that 20 percent had folders that were open to all employees, almost two-thirds of companies had 1,000 or more files open to every employee, and 39 percent of companies had over 10,000 "stale but enabled" user accounts, all of which unnecessarily increase the attack surface.[11] If you're not applying least privilege and are unsure where to begin, start by using role-based access control, which determines users' privileges based on their job or assigned task.
- **Enforce related security principles.** Using need to know and separation of duties in conjunction with the principle of least privilege refines privileges granted to subjects, further reducing risk.
- **Limit the number of privileged accounts.** Because system administrators have virtually unlimited privileges, attackers frequently target those accounts, so limit administrators to the lowest number necessary, preferably fewer than 10 percent of total users. Any more than that increases both the risk and the amount of work required to oversee and monitor logs.[12] In addition, grant standard users local administrator rights only when absolutely necessary.
- **Disable unnecessary components.** When configuring new systems or applications, remove or disable all unnecessary services, which are often enabled and running by

default at start-up. Should someone discover vulnerabilities in those components in the future, you won't be at risk.

- **Review logs frequently.** Log and monitor all authentications and authorizations to critical systems and review logs *daily*, if feasible. Use automation to summarize common events and alert you to anything unusual. Look for both successful and failed login attempts as well as any type of access control changes, for example, newly added firewall rules or user accounts that were added without prior management approval.
- **Regularly reevaluate accounts and privileges.** If possible, review privileges monthly or, at a minimum, quarterly. Ensure active accounts have the minimum privileges required, revoke any excess privileges, and properly terminate any old or inactive accounts. Regular review helps eliminate "privilege creep," which often occurs when departments reorganize or individuals change roles and subjects retain privileges they no longer need. A common nonuser example is a firewall that has pages and pages of years-old, project-specific rules that have never been cleaned up.
- **Use time-limited privileges.** As much as possible (without impeding an employee's ability to do their job), grant privileges just long enough for a subject to perform a specific task (such as a user changing a password or, as mentioned earlier, a manager completing a performance review). Whenever feasible, do the same for specific administrator tasks to reduce the threat window.

Reduce the Security Risks from Privileged Users in 6 Ways

Quick question. How many Windows administrator accounts exist in your company? Lots of them? Then it's likely that many of these privileged accounts are used by individuals who don't need this level of access to perform their role; or who only need privileged access for one or two tasks.

The truth is, providing full admin rights to users who aren't trained as IT system administrators increases security risk and manageability costs and makes it difficult to achieve compliance. This blog briefly presents six simple restrictions that, when combined, will: 1) reduce the likelihood an individual will inadvertently change some administrative settings and require IT assistance to fix the issue; and 2) make it more difficult for an individual to alter or disable certain protections on your endpoints.

For even better protection, your long-term goal should be to change any unnecessary administrator accounts to standard user accounts and employ a least privilege approach.

Six Simple Restrictions

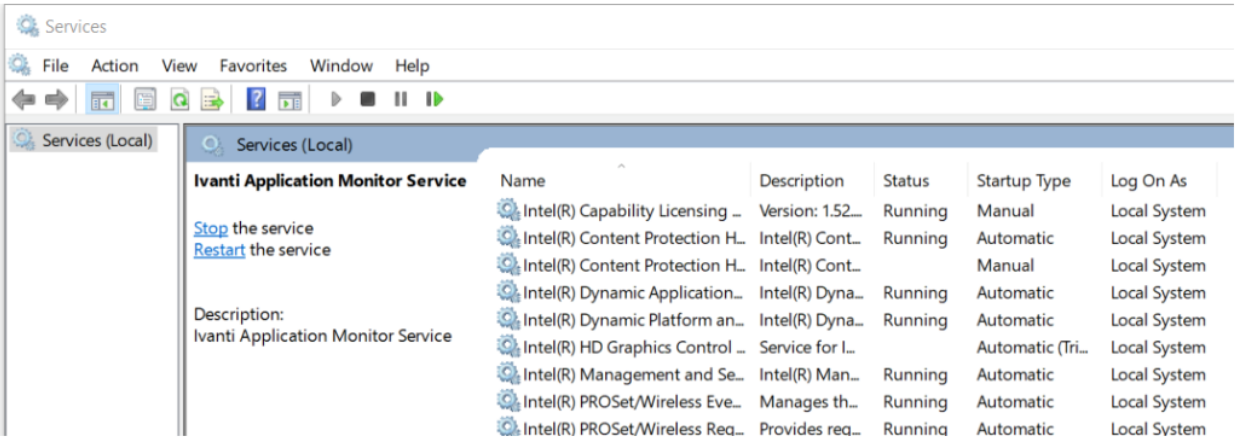
1 – Prevent Users from Changing the UAC Setting

Ivanti advises that all your end-users, including those with admin accounts, employ User Account Control. Microsoft states on its website: *"User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop."*

It's advisable that UAC is active on all machines, with the Always Notify setting selected. This is set via group policy. Ivanti Security Controls can prevent administrators from turning off User Account Control.

2 – Prevent Users from Running the MMC with Admin Privileges

Microsoft's management console (MMC) is a framework that provides end-users with an interface for management and configuration of the operating system. It allows the end-user to load snap-ins. Each snap-in is a tool to manage a particular Windows feature, e.g., the Services snap-in provides a tool to manage Windows services.



This can be very powerful. For example, in the Services snap-in, an end-user with admin privileges can stop services. If a stopped service was part of your antivirus software, it could disable antivirus scanning on any downloads, increasing the threat from malware. With Ivanti Security Controls, you can prevent end-users with administrator accounts from running the MMC with administrator privileges.

3 – Prevent Users from Running Commands or Scripts with Admin Privileges

Windows supports some alternative ways to interact with the operating system by issuing specific commands via command line interpreters or by executing scripts. The former is used for management purposes and the latter is typically used for automation. The command line interfaces that come with Windows are the Command Prompt and Windows PowerShell. Also included with the operating system is the Windows Script Host that can be used to run scripts in a variety of scripting languages.

Anyone with administrative privileges can execute commands or scripts, and this provides an alternative method in many cases to override the GUI-based restrictions mentioned in this blog. For this reason, the command line interpreters and the Windows Script Host should be restricted. The application-control capabilities in Ivanti Security Controls can help with this.

4 – Prevent Users from Being Able to Edit System Settings in the Registry

The Windows registry is important because it stores vital information about a Windows endpoint and its configuration, as well as information about all application programs that are installed. By offering the ability to directly access and change registry keys, admin privilege allows end-users to navigate around central management policies whenever they choose and change the settings. This access provides another route for users to circumvent many of the protections described in this blog. Ivanti Security Controls can be used to restrict privileged access to the registry or to block access to the registry entirely.

5 – Prevent Users from Disabling or Changing Endpoint Firewall Settings

A firewall is a network-security device that monitors traffic to or from your network and allows or blocks traffic based on a defined set of security rules. Firewalls make it more difficult for malicious software to spread throughout a network.

If you're using the Windows Defender firewall, then preventing this functionality from being disabled is recommended. You can do this using Ivanti Security Controls.

6 – Prevent Users from Elevating Applications that Could Introduce Malware

End-users with admin privilege can launch any application with elevated privileges. Some of these applications—email and browser applications, for example—can introduce malware to an endpoint. If one of these applications is running with admin privilege, then any child processes spawned containing malware would also run with admin privilege. With Ivanti Security Controls, you can restrict these applications so that they only ever run with standard privileges.

Information Current as of 11/30/2021

Sources:

https://www.techtarget.com/searchsecurity/definition/privilege-creep

https://www.beyondtrust.com/blog/entry/don-t-fall-victim-to-privilege-creep

https://www.f5.com/labs/articles/education/what-is-the-principle-of-least-privilege-and-why-is-it-important

https://www.ivanti.com/blog/six-ways-restrict-end-users-admin-privileges