Securden

Overcoming the security risks associated with local admin accounts

White Paper

Abstract

The all-powerful local administrator accounts in Windows carry significant security risks, and improper management could lead to disastrous situations. It is believed that more than 90 percent of the security vulnerabilities in Windows arise due to local admin rights. From a security perspective, though local admin accounts by themselves don't cause issues, not managing them properly leads to serious repercussions. This white paper analyzes the common practices in managing local admin accounts, the associated security risks, the strategies to mitigate the risks, and the comparative merits and demerits of different approaches.

Table of Contents

Local admin accounts and security risks

We are all too familiar with the local administrator account that gets created automatically when installing a Windows computer. The local admin is all too powerful but restricted only to that local computer. The account offers complete control over files, folders, services, and local user permissions management. The local admins can install any software, modify or disable security settings, transfer data, and create any number of new local admins.

Local accounts with administrator privileges are considered necessary to be able to run system updates, software upgrades, and hardware usage. They are also helpful to gain local access to machines when the network goes down and when your organization faces some technical glitches.

From a security perspective, local admin accounts by themselves won't cause major issues. But not managing them properly can have serious repercussions. We live in a period where social engineering attacks are used as a primary mode to trap people to fall prey and expose their credentials. All that a hacker needs to execute a massive attack is gaining access to a local admin account. It takes just one compromised Windows host for an attacker to move laterally in your network and wreak havoc.

Over 90% of the vulnerabilities in Windows arise due to local admin rights. Why is it so?

Before analyzing the security risks associated with improper management of local admin accounts, let's review some common practices.

Do you know the number of local admin accounts you have in your organization?

Most likely, the answer would be 'no.' You are not alone. Even some very large organizations with mature security models do not have this visibility. Consider a Windows environment with hundreds of machines. If there is no visibility on the number of local admin accounts and how they are being used, it is undoubtedly the starting point for major security issues.

One password to unlock any local admin account

It is very common to see the same password assigned to all/most local administrator accounts in the organization. It makes the life of IT staff and helpdesk technicians very easy. When Windows machines are deployed in bulk, sometimes the configuration is done by creating a Windows image with a local admin account. The image is pushed on all machines.

When doing so, all the machines get the same password, which is usually ignored or forgotten. A few other organizations follow the practice of assigning identical passwords that follow a set pattern. When one password is known, it is not tough to guess other passwords. All that hackers need is just one local admin password.

Let's now take a deep look into some of the security risks.

Pass-the-hash attacks and lateral movement

Windows caches the passwords as hashes to facilitate single sign-on. If an attacker gains access to a system (say, through a social engineering attack), all that is needed is to pass the hashes. The attacker need not even try to get the password in plain-text. Hash dump tools like Mimikatz will get them the hashes. Just the hash is enough for successful authentication. If the hacker could get the hash of one local admin account, lateral movement becomes easy as most of the devices are assigned with the same password.

The situation becomes worse if the machine was previously accessed using domain administrator credentials. The attacker could get the hashes of the domain admin credentials.

Risk of malware entry

The most typical malware transmission modes are the installation of unapproved software, downloading an email attachment, and visiting malicious websites. Most of the malicious software generally runs with the same rights as the user who is logged on. Local admin rights allow the code to be run on local machines with full privileges without user notifications exposing the organization to a broader attack. Malware generally requires elevated privileges to gain a foothold on machines.

Bypass security settings, run exploit code

The all-powerful local admin access allows hackers to bypass critical security settings, delete system logs, impersonate other logged-on accounts, run exploit code or tools, and eventually gain access to sensitive data. If the system runs applications with system privileges (typically scheduled tasks running applications and processes), attackers could simply attach malicious software to the existing applications and run them silently. Not just external hackers, even an internal user with malicious intent could try to attack if your organization password policies are weak or not appropriately managed.

These are just a few examples of the major security risks and attack patterns. The possibilities are endless and limited only to the imagination and technical expertise of the hacker.

Time and again, hackers are seen exploiting weaknesses and vulnerabilities in the configurations related to local admin accounts. What do we need to do to protect?

How do we mitigate the security risks?

It is evident that local admin accounts carry significant security risks, and improper management could lead to disastrous situations. In sophisticated attacks, hackers dwell undetected for a prolonged time.

The mitigation strategy could be approached from two perspectives:

1. **Eliminate the local admin accounts altogether; make everyone a standard user.** But this approach leads to the introduction of the 'request-approval' concept. Employees might have to wait for permissions resulting in delays, productivity loss, and frustrations. Is there a way to eliminate local admin accounts, overcome these hurdles and make the process seamless?

2 **Retain the accounts, manage them properly.** While this approach proves to be very convenient, it requires careful planning, management, and maintenance to mitigate the risks. The passwords should be strong, unique, and periodically changed. Endusers should be educated about the implications of their activities as local admin and the associated security risks. Is there a way to automate the management of the local admin accounts and reduce the risks?

Mitigation Strategy 1:

Let us analyze the second approach first. While retaining the local admin accounts, how to enforce the best practices?

When deciding to retain the local admin accounts, the foremost thing to be done is to minimize the number of local admin accounts - unnecessary accounts should be removed. Then a strong password policy should be enforced. You shouldn't end up storing the passwords on text files or spreadsheets. Managing passwords manually is next to impossible and a major security risk in itself. There are two ways in which you can properly and efficiently manage the local admin accounts.

1. Using Microsoft Local Administrator Password Solution (LAPS)
2. Deploying a Privileged Account Management (PAM) Solution

Before getting into the details, let us examine the various efforts made by Microsoft in managing privileged access.

Microsoft's efforts to managing privileged access

A vast majority of vulnerabilities in Windows environments are related to the local admin accounts. Microsoft was obviously concerned about this fact and made sincere efforts to find a solution. First, they came up with the concept of User Account Control (UAC),

which allowed administrators to log on to workstations with standard privilege and then use "Run as" to elevate rights on-demand. UAC, no doubt, was a brilliant concept, but it too was susceptible to pass-the-hash attacks, besides introducing several operational challenges.

Another significant approach was the Privileged Access Workstation (PAW), which involves separating administrative accounts from normal user accounts - physical separation of standard and privileged access. PAW requires users to access privileged accounts from a dedicated, hardened, locked-down device that is only used for privileged activities. PAW is not to be connected with the internet and won't accept inbound connections. PAW implementation is not something that is simple and straightforward. It also introduced the burden of maintaining a separate infrastructure. User experience was severely constrained.

Of all the attempts by Microsoft, perhaps the most successful one is the introduction of the Local Administrator Password Solution (LAPS). LAPS enables IT organizations to randomize the passwords of domain-joined local administrator accounts at periodic intervals. This ensures that the local admin accounts are assigned with strong, unique passwords that are periodically changed.

Let us now examine the benefits and limitations of Microsoft LAPS

LAPS revolves fully around the Active Directory to manage the passwords of local administrator accounts. The local admin passwords are centrally stored in the Active Directory against the respective machine objects. Authorized users can retrieve the passwords when access is needed.

Through Group Policy, LAPS enforces strong, unique password usage. LAPS automatically identifies password expiration and generates a new password. Even if an attacker gains access to one local admin account, chances of lateral movement become remote. This saves your other endpoints and accounts in your network from attacks.

Simplicity - both a strength and weakness of LAPS

LAPS is very simple. It is tied to the AD and can manage local administrator accounts passwords. Nothing more. So, this simplicity is both a strength and a weakness. Its scope is too narrow.

Some of the limitations are:

- LAPS covers only domain-joined accounts
- True to its name, it covers only local admin accounts. In order to stay ahead, organizations are moving towards increased automation of their services with very little human intervention. In addition to person-user accounts, non-person (Machine accounts) high privilege accounts such as your service, domain, application, or database accounts also need protection as well.
- It doesn't cover non-Windows environments. Enterprise environments typically have UNIX, MacOSX, and other types of devices that involve privileged access.

While LAPS serves as a great tool to manage only the local admin accounts, it doesn't fit the needs of most organizations, which are required to secure privileged access in its entirety.

This is where the Privileged Access Management (PAM) solutions come into the picture.

Privileged Access Management (PAM) for holistic security and controls

LAPS is undoubtedly a great solution. But its usage is strictly limited to local admin accounts. It cannot offer holistic privileged access security much needed by the enterprises. A comprehensive PAM Solution can help you take total control of privileged access, including local admin access across the organization. PAM solutions deal with all aspects of privileged access - centrally controlling, auditing, monitoring, and recording all access to critical IT assets.

Some of the significant advantages of PAM solutions include:

- Automatic network scans and accounts discovery
  - Discover all the privileged accounts on disparate systems and devices. It will unearth even long-forgotten accounts, accounts not in use, etc.

- Consolidate all privileged accounts in a secure repository for centralized management and controls

- Manage domain admin, service accounts
  - Manage the all-important domain admin accounts.
  - Track and manage the Windows domain accounts are used to run services, processes, scheduled tasks, and IIS app pools.

- Manage non-human accounts and machine identities
  - Manage SSH keys, DevOps secrets

- Randomize passwords periodically
  - Randomize passwords of local, domain, service, and application accounts periodically. Ensure strong, unique passwords.

- Just-in-time access
  - Ensure just-in-time access to devices and applications through automated workflows
  - Grant remote access to devices and applications without showing the passwords to users, third-parties.

- Monitor activities, record sessions
  - Monitor privileged sessions in real-time. Terminate session if malicious activity is found.
  - Record sessions, playback whenever required.

- Maintain audit trails, generate actionable reports
  - Maintain a complete trail of activities and trace 'who' did 'what' and 'when'.
  - Gain organization-wide visibility and actionable security insights on IT access through analytical reports.

From the foregoing, it is clear that organizations require a full-featured PAM solution for holistic security.

We have discussed how to automate the best practices when you decide to retain the local admin accounts. Let us now analyze the merits and demerits of the other approach - eliminating the local admin accounts altogether.

Mitigation Strategy 2:

Eliminating local admin rights altogether

One of the most effective approaches to reducing risks is eliminating the local admin accounts altogether and making everyone a standard user. But this approach leads to the introduction of the 'request-approval' concept, which is inefficient. Employees might have to wait for permissions resulting in delays, productivity loss, and frustrations.

This leads to the pertinent question: Is there a way to eliminate local admin accounts, overcome these hurdles and make the process seamless?

Yes, absolutely!

Local accounts with administrator privileges enable users to carry out software installations, change certain system settings and perform many other tasks without relying on help desk technicians and system administrators. When local administrator rights are removed, striking a balance between security and productivity becomes critical. This is where endpoint privilege management solutions come into the picture.

Endpoint privilege management basically relates to removing local administrator rights on Windows endpoints and elevating applications for standard users. The most important aspect here is that the privileges are NOT elevated for users; only the applications and processes are run with privileges. Users will always remain standard users.

Local admin rights removal goes together with application control

While removing the local administrator rights forms just one part of the process, the other part relates to establishing a policy-based application control process. Administrators should be able to define and control which applications/processes can be run by standard users. This, in turn, leads to whitelisting trusted applications and preventing unapproved and malicious applications. This empowers standard users to seamlessly run approved applications (that would normally require admin rights) whenever needed.

There may be occasions when specific users would require broader privilege. There may be contingencies that would mandate full access to certain users. There should be provision for granting a time-limited, fully controlled, and comprehensively audited temporary administrator access on a need basis. Such access should be controlled by a well-defined workflow, which would take care of automatically revoking the access.

How does eliminating local administrator rights help reduce risks?

From an IT security perspective, eliminating local administrator rights on endpoints presents multiple benefits:

- As discussed earlier, over 90% of critical vulnerabilities in Windows are stated to be related to local admin privileges. This crucial security gap could lead to major breaches and could be easily mitigated by removing local admin rights. Least privilege enforcement on endpoints is now a necessity.
- Malware quickly and easily spreads through the installation of unapproved software, pirated tools, opening malicious email attachments, clicking malicious URLs, visiting harmful pages (drive-by downloads), and so on. Even tech-savvy end-users can unintentionally fall prey to any of these attacks and malware would gain a strong foothold. In the absence of admin rights, users will be able to run only approved applications and processes. You can prevent the installation and use of unapproved software and thereby block malicious software from getting into the organization. This significantly reduces the risk of malware or ransomware.
- Removal of local administrator rights helps enforce least privileges across the organization. You can ensure that all your users have just enough access to the IT infrastructure. This, in turn, helps in significantly arresting the lateral movement of hackers who happen to gain a foothold on one machine.
- In short, by eliminating local admin rights, you can significantly reduce the attack surface.

It is clear that eliminating local administrator rights is the best practice approach. How do we implement a least privilege model without impacting productivity?

This is where privilege management solutions like Securden Windows Privilege Manager come into the picture. Manual approaches could at best help you eliminate administrator rights. But only a policy-based, automated approach can help you achieve application control and ensure that user experience is not adversely impacted. Without the right tool, elevating applications, processes, scripts, and tasks for standard users could be counterproductive and frustrating.

How does Securden Windows Privilege Manager help?

Securden Windows Privilege Manager helps you to eliminate local admin rights without impacting productivity. It seamlessly elevates applications for standard users. Through robust workflows and policy-based controls, end-user experience remains the same even when administrator rights are removed. Securden makes the process seamless and scalable.

Granular application control, robust policy-driven approach

You can elevate administrator privileges to trusted applications for standard users through a fully policy-driven approach. Basically, you will whitelist applications, create policies and associate them with users and devices for seamless elevation on-demand. You will have granular control on which applications are to be elevated on specific endpoints, and by specific users or groups.

- You can enforce policies without impacting end-user productivity.
- You will also reduce the workload of your IT in managing endpoint privileges.

Seamless end user experience, various options

Even when local admin rights are removed, end users will be able to perform their activities without any interruption.

- They will be able to run the whitelisted processes and applications without requiring any approvals.
- For installing/running new applications, Securden provides a self-service portal for standard users to get approval for application elevation well in advance or whenever needed.

- When broad administrative privileges are required to meet specific requirements, users can raise a request and get approval for temporary administrator access. The lightweight agent that sits at the endpoints grants elevation just-in-time and for a limited duration after security controls. At the end of the approved time, Securden revokes the privilege and automatically closes the elevated applications. It also records and reports the list of applications elevated during the session.

Continuous monitoring, complete control

One of the critical requirements mandated by various IT regulations is continuously monitoring the privileged access scenario. Even when the least privileges are enforced, organizations should be able to demonstrate the same. It requires continuously tracking and reviewing user access entitlements, and auditing activities.

- Securden records all user activities, including the applications elevated and run by standard users.
- It also tracks the creation of new admin accounts and shows them in reports.
- You can also review the membership of various privileged AD groups from Securden itself and manage membership.

In summary, to reduce the risks associated with local admin accounts, you should carefully consider the mitigation strategies. The two options you have are: Eliminate the admin rights altogether or manage them properly. And whatever option you choose, you need the right solution. Check out Securden Windows Privilege Manager and Securden Unified PAM.