Remote Use of Local Accounts: LAPS Changes Everything

By kexugit

Archived: 2026-04-06 03:21:20 UTC

Long overdue post revisiting the question about whether and when to block the use of local accounts, particularly for remote administration.

Beginning in 2014 with our baselines for Windows 8.1 and Windows Server 2012R2, our security baselines have been blocking remote use of local accounts. Back then, Windows had yet to offer anything resembling secure management of administrative local account credentials. It was typical for an entire organization to have an administrative local user account with the same username and password on every Windows computer. One problem with that is that the common password often becomes a well-known secret over time with no way to revoke access from anyone who ever received it. But by far the biggest problem is that an attacker with administrative rights on one machine can easily obtain the account's password hash from the local Security Accounts Manager (SAM) database and use it to gain administrative rights over the other machines using "pass the hash" techniques.

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS). LAPS is an elegant and lightweight mechanism for Active Directory domain-joined systems that periodically sets each computer's admin account password to a new random and unique value, storing the password in a secured confidential attribute on the corresponding computer object in Active Directory where only specifically-authorized users can retrieve it.

LAPS changes everything.

Not only does LAPS neutralize both the pass-the-hash and well-known-secret problems, it creates new opportunities for remote management. With LAPS – or in fact, with any solution that makes local account passwords unique and not guessable – using local accounts for remote computer management actually offers some advantages over using domain accounts. They can, that is, provided that their use isn't blocked by security policy – which our baselines do today.

It's all about credential hygiene. Good credential hygiene means not exposing credentials on a potentially-compromised system when those credentials can be used to compromise another system. Credentials can be a plaintext password, an account's NTLM hash, or a Kerberos TGT. Microsoft's Pass the Hash whitepapers go into detail about which remote logon types and tools expose credentials and which ones don't.

Let's say your helpdesk technicians each have a domain account that is granted administrative rights on all workstations in the domain. User Umberto reports computer issues, so Helen helpdesk technician logs on remotely to the workstation using her privileged domain account, not realizing that the workstation has been compromised with credential theft malware. Depending on how Helen logged on, her account credentials could be stolen and the thief can now gain administrative control over all workstations. All the technicians might follow the whitepapers' recommendations, but they must do it the right way every single time. One technician with a privileged account making one mistake just one time can lead to a domain-wide compromise.

Let's say instead of using a privileged domain account, Helen helpdesk technician retrieves the LAPS password for the workstation and uses the LAPS-managed administrative local account to log on. Credential theft is not a problem. If the thief gets the hash or even the plaintext password, it's useful only on the computer that the thief already controls. So Helen can use whichever logon type or remote tool is most convenient for the work being performed.

Note: One caveat about using remote desktop: do not enable drive redirection for your local volumes when connecting to a potentially-compromised system. And avoid clipboard redirection as well. This caveat applies whether you're using a LAPS-managed account, /restrictedAdmin, or anything else.

If you have deployed LAPS or another local account password management solution and you want to use local accounts for the remote administration of Windows computers, you need to change three of the Computer Configuration settings that we recommend in the baselines for Windows client and Windows Server in the Member Server role. We recommend these changes only if you plan to use LAPS-managed local accounts for remote administration. Note also that the local-policy scripts included with the Windows 1803 and 1809 baseline packages include "Non-Domain" options that implement these same changes.

Policy path	Windows Settings\Security Settings\Local Policies\User Rights Assignment
Policy name	Deny access to this computer from the network
Baseline setting	*Win client*: NT AUTHORITY\Local Account *Win Server*: NT AUTHORITY\Local account and member of Administrators group
Updated setting	[empty]

Policy path	Windows Settings\Security Settings\Local Policies\User Rights Assignment
Policy name	Deny log on through Remote Desktop Services
Baseline setting	NT AUTHORITY\Local Account
Updated setting	[empty]

Policy path	Administrative Templates\MS Security Guide *(*)*
Policy name	Apply UAC restrictions to local accounts on network logon
Baseline setting	Enabled
Updated setting	Disabled

(*) “MS Security Guide” is a collection of custom settings that comes with the security baselines and is represented in SecGuide.admx. You can configure the updated setting directly by configuring the registry value LocalAccountTokenFilterPolicy to REG_DWORD value 1 in HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- **Anonymous**
  December 11, 2018
  Hi Aaron,a benefit of a 'no remote logon' policy is it's definitive; no matter what local accounts get setup, whether by the end-user or a helpful desktop admin, you're guaranteed they can't be used remotely. LAPS only targets the (500) local admin and doesn't give any management of other local accounts.LAPS is a good solution, but it needs a bit more to provide that same definitive protection, something like a new SID "Local Accounts Not in LAPS", or "Local accounts in admin group but not the administrator" which could be used in the "Deny*" security policy GPOs.*[Aaron Margosis] A clarification: LAPS manages one administrative local account, which doesn't necessarily have to be the -500 built-in admin.More: there's no good reason to have multiple administrative local accounts on an enterprise system. They would each have full control over the other. You have no reliable auditability, so you might as well have just one such account.More: users need admin rights to create local accounts, and if they're doing things like that on your systems, you've got bigger security issues. They can open all kinds of unaudited mechanisms for remote control. Enterprise users shouldn't have admin rights.*
- **Anonymous**
  January 18, 2019
  Using the Administrator account can be a good choice for desktops and laptops.However, the drawback of everybody using the same local account is that it's more difficult to know who did what...Furthermore, this is an all or nothing approach: you are either a user or an administrator.On servers, I would rather apply the principle of least privilege with JEA.Anyway, thanks for this interesting reminder about LAPS!
