
NT KONF
25. – 27.
SEPTEMBER
2023
PORTOROŽ
NT KONF
NT KONFERENCA

All new and cloudy Windows LAPS!

Tomislav Fučkar, APIS IT d.o.o.

Who is this guy?

Tomislav Fučkar MCSA, MCSE, CCNA, RHCSA

- Over 30 years of experience with Microsoft products
- Actively working with: AD, Entra ID, PKI, PAM (CyberArk), PowerShell
- Trainer at Algebra d.o.o.
- Fields od interest: Identity & Security
- Hobby: photography
- Sport: tennis

What is LAPS and why should I use it?

- LAPS stands for “Local Administrator Password Solution”
- LAPS manages local account passwords of domain-joined computers, ensuring that they are regularly updated and unique
- The passwords managed by LAPS are stored in Active Directory (AD), protected by Access Control List (ACL) and (optionally) encrypted
- Only eligible users can read the password information or request its reset, enhancing the security of local accounts

What's new in Windows LAPS

- Windows LAPS is now a built-in feature of Windows
- Supports Microsoft Entra ID (ex Azure Active Directory)
- Retrieves stored passwords via Microsoft Graph
- Supports password history (keeps last 3 passwords)
- Supports DSRM password rotation
- Supports Automatic Password Rotation: The feature automatically rotates the password after the retrieved password is used
- Can be managed via GPO or Intune

(New) Windows LAPS Powershell cmdlets

- Get-LapsAADPassword
- Get-LapsADPassword
- Get-LapsDiagnostics
- Find-LapsADExtendedRights
- Invoke-LapsPolicyProcessing
- Reset-LapsPassword
- Set-LapsADAuditing
- Set-LapsADComputerSelfPermission
- Set-LapsADPasswordExpirationTime
- Set-LapsADReadPasswordPermission
- Set-LapsADResetPasswordPermission
- Update-LapsADSchema

Requirements

- Supported client OS's: Windows 10, Windows 11
- Supported server OS's: Windows Server 2019, Windows Server 2022
- April 2023 security update must be applied
- Windows Server 2016 DFL (or later) needed for password encryption and DSRM password management

	Clear-text password storage supported	Encrypted password storage supported (for domain-joined clients)	DSRM account management supported (for DCs)
Below 2016 DFL	Yes	No	No
2016 DFL with one or more WS2016 DCs	Yes	Yes	Only WS2019 and later DCs
2016 DFL with only WS2019 and later DCs	Yes	Yes	Yes

Things to know…

Entra ID Roles with permission to read passwords:

- Global Administrator
- Cloud Device Administrator
- Intune Service Administrator

Registry locations:

- Intune managed: HKLM:\SOFTWARE\Microsoft\Policies\LAPS
- GPO managed: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS
- Local config: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config
- Legacy: HKLM:\SOFTWARE\Policies\Microsoft Services\AdmPwd

Event Logs location:

- Application and Services > Microsoft > Windows > LAPS > Operational

Things to remember…

- Windows LAPS needs schema extension (Update-LapsADSchema)
  - Don’t forget to run „Refresh directory schema” in Azure AD Connect afterwards ☺
- Regardless of the way devices are managed (GPO or Intune), you can configure passwords storing in Active Directory or Entra ID
- If password backup location is Active Directory, devices will ignore LAPS profile in Intune (if configured)

DEMO

Thank you!

...questions?

25. – 27.
SEPTEMBER
2023
PORTOROŽ

This is not school, but we love to get grades.
Please fill out our questoineers and leave us your feedback.
You may even win some cool rewards.

NT KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ