

WINDOWS LAPS.



Windows LAPS gives every device its own local administrator password, rotates it on a schedule, and backs it up to Active Directory or Microsoft Entra ID where only authorized roles can read it. **It exists because one shared local admin password turns a single compromised machine into all of them.**

- ONE PASSWORD PER DEVICE
- ROTATE ON A SCHEDULE
- ENCRYPT IN THE DIRECTORY
- RESET AFTER USE

01 THE MECHANISM



The Problem: One Hash, Every Machine

Local administrator accounts often share one password across many devices, and attackers exploit that to move laterally: pass-the-hash authenticates with the stolen hash and never needs the clear text. **Same password, same hash, every device.** [01] [09]



The Fix: A Unique, Rotating Secret

Built into Windows since the April 11, 2023 updates. When the managed password expires, the device generates a new random one that meets policy, stores it in the directory with its expiration time, and rotates again when that time arrives. **Defaults: 14 characters, four character classes, every 30 days.** [02] [03]



The Guard: Who Can Read It

In Active Directory the password sits on the computer object behind ACLs and, by default, AES-256 encryption only Domain Admins can undo. In Entra ID, by default only Global, Cloud Device and Intune Administrators retrieve it. **Retrieval is a privileged, audited act.** [02] [05]

02 THE FLOW

Deploy It DESIGN

- Prepare the directory:** AD: run Update-LapsADSchema once per forest, grant computers self-write on their OU with Set-LapsADComputerSelfPermission, and check Find-LapsADExtendedRights for who can already read confidential attributes. Entra ID: enable LAPS in the tenant's Device settings. [04] [05]
- Pick the account:** leave AdministratorAccountName empty and LAPS manages the built-in account by its well-known RID, whatever its name. On Windows 11 24H2 and Server 2025, automatic account management creates and controls a custom account (default WLapsAdmin); Microsoft recommends it, with the built-in Administrator disabled. [04] [06]
- Set the policy:** BackupDirectory 1 (Entra ID) or 2 (AD), encryption on, PasswordAgeDays (minimum 1 for AD, 7 for Entra), length up to 64 or a passphrase, and the post-authentication delay. Intune CSP for Entra-joined devices, Group Policy for domain-joined; CSP overrides GPO. [03]

Run It OPERATE

- Rotate:** a background task wakes every hour (fixed, not a scheduled task). AD-joined devices poll the directory for the expiration time; Entra-joined devices keep it locally. Force it early with Reset-LapsPassword, the CSP ResetPassword action or, AD only, an expiration-time change. [02] [04]
- Retrieve, then let it burn:** Get-LapsADPassword or the Users and Computers LAPS tab for AD; Get-LapsAADPassword, Graph or the Entra and Intune portals for the cloud. Once the account authenticates, the grace period (default 24 hours) ends in a reset and sign-out. [04] [05] [03]
- Watch:** the LAPS Operational channel: 10018 stored in AD, 10029 stored in Entra ID, 10027 rejected by local password policy, 10031 tampering blocked. Filter Entra audit logs for "Recover device local administrator password"; put Conditional Access on the retrieval roles. [11] [04] [05]

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Uniqueness	A random password per device, never shared, regenerated on a schedule: 8–64 characters in four classes, or passphrases on Windows 11 24H2 and Server 2025.
Storage Protection	AD: computer-object ACLs plus AES-256 encryption to one principal (Domain Admins by default; 2016 functional level) with encrypted history. Entra ID: extra encryption plus role-based access.
Bounded Use	Post-authentication actions reset the password and end sessions or reboot after the grace period; expiration protection and tampering protection guard the account.
Accountability	Read and expire rights are granted explicitly per OU; Entra retrieval needs deviceLocalCredentials/password/read; every update and recovery is audited.

04 LOCAL ADMIN CONTROLS COMPARED

CONTROL	STOPS LATERAL REUSE?	WHAT IT LEAVES OPEN
One Image, One Local Admin Password	No	One captured hash authenticates to every device built from the image: classic pass-the-hash.
Rename or Disable the Built-in Administrator	No	The RID-500 SID survives renaming, safe mode can re-enable the account, and other shared admins stay shared.
Deny Network and RDP Logon to Local Admins	No	Blocks remote reuse, but the shared password stays valid at the console and in any script or image.
Legacy LAPS or Emulation Mode	No	Unique, rotated passwords stored in clear text that any extended-rights holder can read; no history.
Windows LAPS With Encryption and Post-Auth Reset	Yes	Closes cross-device reuse; still one account per device, privileged retrievers, and no password after an Entra device is deleted.

WINDOWS LAPS.

ROTATE · ENCRYPT · RETRIEVE

05 PROGRAM OPERATIONS

Manage the account by RID, never by name.

The built-in account's name varies by locale and can be renamed; LAPS finds it by its well-known relative identifier. A custom account must exist before manual mode can manage it, or let automatic mode create it. [04] [06]

Layer the Active Directory permissions.

Outer ring: who may set expiration (sensitive but nondestructive). Middle: who may read passwords. Inner: who may decrypt, Domain Admins unless a wrapper group is the encryption principal. Match the rings to device sensitivity: help desk on frontline machines, not executive laptops. [02]

Pair LAPS with the deny rights and UAC filtering.

Deny network and Remote Desktop logon to “Local account and member of Administrators group”, and keep LocalAccountTokenFilterPolicy at 0 so remote logons with local accounts get a filtered token. ATT&CK lists both as pass-the-hash mitigations. [08] [09]

Retire legacy LAPS and respect “always on”.

The legacy product is deprecated from Windows 11 23H2 and its installer blocked; never let legacy LAPS and Windows LAPS manage the same account, and treat emulation mode as a clear-text stopgap. Windows LAPS enforces policy the moment it applies, so keep new builds in a staging OU or it rotates the deployment account mid-task. [01] [07] [02]

06 CONTROL MAPPING

ATT&CK MITIGATIONS

T1550.002 Pass the Hash: M1026 limit credential overlap across systems, M1052 UAC restrictions on local accounts at network logon, M1018 no domain user in local Administrators on many systems. T1078.003 Local Accounts: M1027 unique local admin passwords; M1026 names LAPS. [09] [10]

MICROSOFT GUIDANCE

Three measures for local accounts with administrative rights: enforce local account restrictions for remote access, deny the network logon right to all local Administrator accounts, and create unique passwords, with LAPS the first-listed way. [08]

POLICY DEFAULTS

BackupDirectory Disabled (0), PasswordAgeDays 30, PasswordLength 14, PasswordComplexity 4, PostAuthenticationResetDelay 24 hours, PostAuthenticationActions 3 (reset and sign out), AD encryption on to Domain Admins, history 0, automatic account management off. [03]

ENTRA ID ACCESS MODEL

Cloud Device Administrator and Intune Administrator hold deviceLocalCredentiaals/password/read; Helpdesk, Security Administrator and Security Reader see metadata only. Custom roles and administrative units scope recovery; Conditional Access can require MFA. [05]

07 WHAT THIS DOES NOT SOLVE

Domain Admin Overlap

LAPS covers one local account per device. A domain user who is admin everywhere is the same overlap. Tier it apart. [09]

The Retriever

Read rights reach every device in scope, and the default Entra roles are highly privileged. Scope, MFA, audit. [02] [05]

A Password in Use

A valid password is full admin, and Microsoft says its holder can defeat the post-auth reset. A limit, not a lock. [03]

Deleted or Rolled Back

Delete the Entra device and its password goes too; a snapshot rollback leaves a torn state. Keep history and backups. [05] [02]

08 MYTHS VS. REALITY

MYTH	REALITY
“Renaming Administrator hides it.”	The SID still ends in 500 and is discoverable; LAPS itself locates the account by RID. [08] [04]
MYTH	REALITY
“LAPS is something you download.”	Windows LAPS ships in the OS; the legacy MSI is deprecated and blocked on Windows 11 23H2 and later. [01]
MYTH	REALITY
“A password in AD is safe because AD is.”	Encryption needs a 2016 domain functional level; below it, clear text behind ACLs that extended-rights holders can read. [04] [02]
MYTH	REALITY
“The 30-day rotation is the protection.”	Uniqueness and the post-authentication reset are; a used password lasts 24 hours by default , not 30 days. [03]
MYTH	REALITY
“Hybrid devices back up to both directories.”	One directory only, never both; Entra registered devices are not supported at all. [01] [05]

09 SPEAK THE PROGRAM — KEY TERMS

PASS THE HASH

Authenticating with a stolen password hash, **no clear-text password needed**; the reason shared local passwords are fatal.

RID 500

The well-known relative identifier of the built-in Administrator account; **survives renaming.**

BACKUPDIRECTORY

The LAPS setting that picks the store: **0 disabled, 1 Entra ID, 2 Active Directory.**

ENCRYPTION PRINCIPAL

The single user or group that can decrypt an AD-stored password; **Domain Admins unless set.**

POST-AUTHENTICATION ACTION

What LAPS does after the account is used and the grace period ends: **reset, sign out or reboot.**

EMULATION MODE

Windows LAPS honoring legacy LAPS Group Policy during migration; **clear text only**, no CSE installed.