Welcome!!

To the Modern Endpoint Management Series

Windows LAPS

MODERN
ENDPOINT
MANAGEMENT
SERIES

Niklas Tinner

Oceanleaf.ch

Endpoint Engineer

MODERN ENDPOINT MANAGEMENT SERIES

08.06.2023/12:00 CEST

Agenda

01

Introduction

Why LAPS? What is Windows LAPS?

02

Design topics

Password retrieval / Administrator account

03

Implementation/Migration

Get started or transition

04

Demo slides Azure AD

Enable Windows LAPS for Azure AD

Introduction

Windows LAPS

MODERN
ENDPOINT
MANAGEMENT
SERIES

Windows LAPS

Microsoft LAPS which was known until yet is now renamed to legacy LAPS.
Microsoft recommends to migrate legacy LAPS to Windows LAPS.

Manage, backup and rotate local administrator password

Why LAPS?

Control local admin rights

Protection against pass-the-hash and lateral-traversal attacks

Improved security for remote support scenarios

➔Eliminate general/shared local admins on devices

🛇 AAD Joined Local Admin or Global Admin role
🛇 Modifications to Local user group membership (Account protection)
🛇 Domain admins used for admin use on clients

New features

General

- Native integrated in Windows
- Store password in Active Directory or Azure AD
- Password history
- Post Authentication Actions on/after use of LAPS account
- New PowerShell module

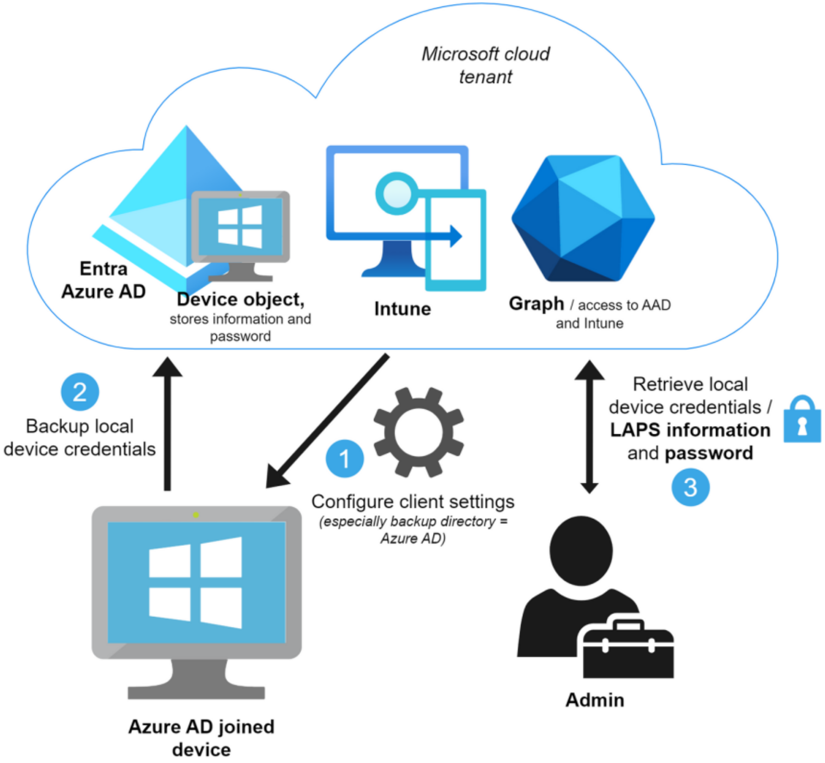
Azure Active Directory

- Integration to Intune (password retrieval & rotate remote action)
- Configuration through Settings Catalog

Active Directory

- New schema attributes
- Domain Services Restore Mode (DSRM) password support for LAPS
- Configuration with GPO
- Support for encryption

Architecture Azure AD


Microsoft cloud tenant
Entra Azure AD
Device object, stores information and password
Intune
Graph / access to AAD and Intune
2
Backup local device credentials
1
Configure client settings (especially backup directory = Azure AD)
Retrieve local device credentials / LAPS information and password
3
Azure AD joined device
Admin

Design topics

Windows LAPS

MODERN
ENDPOINT
MANAGEMENT
SERIES

Password retrieval

Azure Active Directory

- Uses with assigned built-in roles (Intune Admin, Cloud Device Admin or Global Admin) can read the password
- Limit access for admins to a set of devices with Administrative Units

Active Directory

Create an AD group to:

- Configure the **GPO setting** ADPasswordEncryptionPrincipal with an identity that can **decrypt** the encrypted password (If password encryption is enabled)
- Set **AD extended rights** to set permissions on OU level with “Set-LapsADReadPasswordPermission” to read the password

Admin account

⚠ The built-in administrator account of Windows:

- Is disabled by default
- No lockout threshold
- A well-known SID

Note: A security baseline setting would enforce the lockout threshold of the administrator. (default set on 22H2 initial installed systems)

➔ Attackers could brute-force this account.

To address these vulnerabilities and set countermeasures, you can create a dedicated local admin account which will be managed through LAPS.

Implementation/Migration

Windows LAPS

MODERN
ENDPOINT
MANAGEMENT
SERIES

Prerequisites

- OS
  - Windows 10 April 2023 update
  - Windows 11 21H2/22H2 April 2023 update
  - Windows Server 2019 and above with April 2023 update
- Domain functional level 2016+ (for all features)
- License/costs = nothing
- Roles
  - AD > Schema admin and domain admin to configure GPO
  - AAD > Cloud Device Admin and Intune Admin

Scenario

	Active Directory	Azure AD
Backup directory	AD	AAD
Join state	**AD joined** (~~hybrid~~)	**AAD joined** or hybrid
Policy deployment	GPO	Intune settings catalog or GPO
Implementation steps	• Schema update • Set extended rights • Configure GPO settings • GPO for additional admin	• Tenant enablement • Intune settings catalog • Proactive remediation for additional admin ➔ **Demo slides incoming**
Recommended target devices	Windows Server and any on-premises only	All Windows clients

Setup scenario Azure AD

Tenant enablement

Intune settings catalog

Proactive remediation

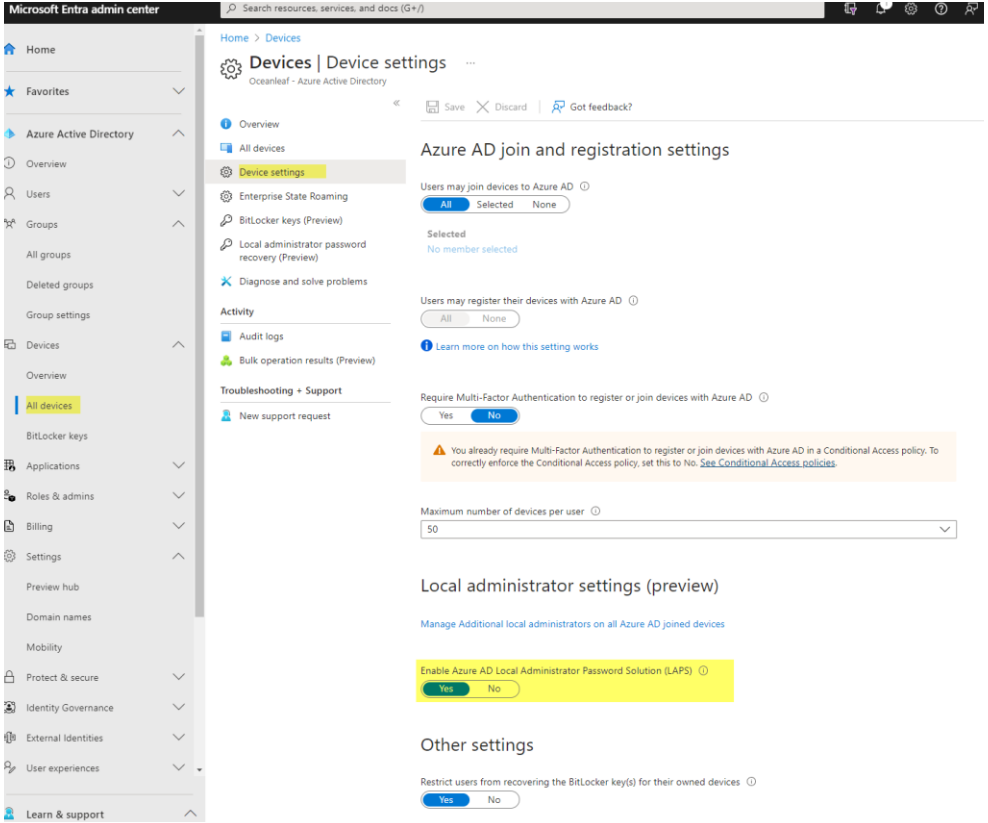
(for additional admin)

Steps:

1. Azure AD>Device settings>
Enable LAPS here

Requirements:

- Cloud Device Admin or Global Admin



Devices | Device settings

Oceanleaf - Azure Active Directory

Azure AD join and registration settings

Users may join devices to Azure AD: [✓ All] Selected None

Selected
No member selected

Users may register their devices with Azure AD: All None

Learn more on how this setting works

Require Multi-Factor Authentication to register or join devices with Azure AD: Yes [✓ No]

You already require Multi-Factor Authentication to register or join devices with Azure AD in a Conditional Access policy. To correctly enforce the Conditional Access policy, set this to No. See Conditional Access policies.

Maximum number of devices per user: 50

Local administrator settings (preview)

Manage Additional local administrators on all Azure AD joined devices

Enable Azure AD Local Administrator Password Solution (LAPS): [✓ Yes] No

Other settings

Restrict users from recovering the BitLocker key(s) for their owned devices: [✓ Yes] No

Setup scenario Azure AD

☑ Tenant enablement

🛠 **Intune settings catalog**

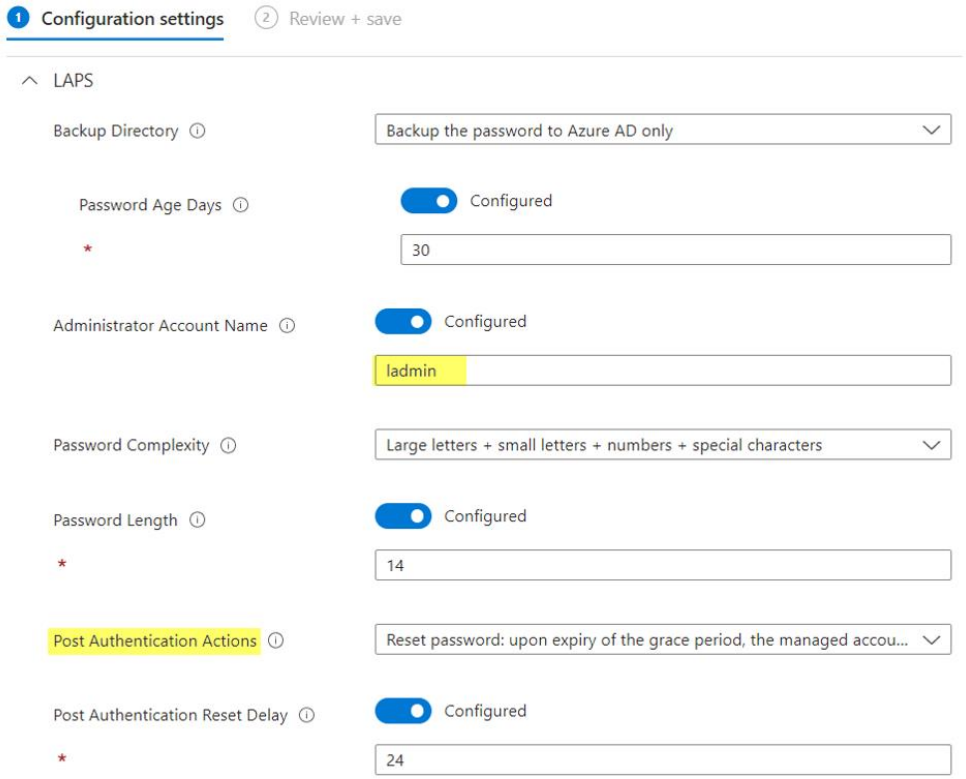
▨ Proactive remediation
(for additional admin)

🚀 Steps:

1. Intune portal>Endpoint Security> Account Protection
2. Create a profile for LAPS
3. Configure settings
4. Assign

ⓘ Requirements:

- Intune admin



① Configuration settings ② Review + save

LAPS

Backup Directory ⓘ: Backup the password to Azure AD only

Password Age Days ⓘ *: Configured — 30

Administrator Account Name ⓘ: Configured — ladmin

Password Complexity ⓘ: Large letters + small letters + numbers + special characters

Password Length ⓘ *: Configured — 14

Post Authentication Actions ⓘ: Reset password: upon expiry of the grace period, the managed accou...

Post Authentication Reset Delay ⓘ *: Configured — 24

Setup scenario Azure AD

MODERN ENDPOINT MANAGEMENT SERIES

☑ Tenant enablement

☑ Intune settings catalog

Proactive remediation
(for additional admin)

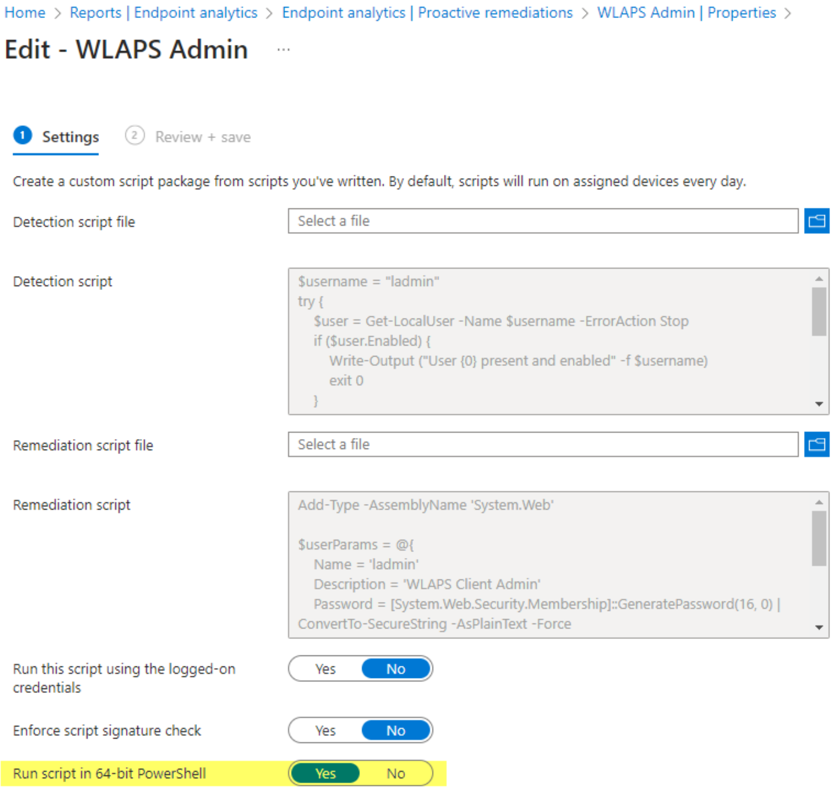
Steps:

1. Intune portal>Device configuration> Remediations>Create script packages
2. Grab script files on my blog (by Nicola Suter)
3. Upload and assign

Requirements:

- Intune admin
- Script files

Detect-CustomAdminAccountExists.ps1 (github.com) and Remediate-CustomAdminAccountExists.ps1 (github.com)



Home > Reports | Endpoint analytics > Endpoint analytics | Proactive remediations > WLAPS Admin | Properties >

Edit - WLAPS Admin

Create a custom script package from scripts you've written. By default, scripts will run on assigned devices every day.

Detection script file: Select a file

Detection script:

```
$username = "ladmin"
try {
   $user = Get-LocalUser -Name $username -ErrorAction Stop
   if ($user.Enabled) {
      Write-Output ("User {0} present and enabled" -f $username)
      exit 0
   }
```

Remediation script file: Select a file

Remediation script:

```
Add-Type -AssemblyName 'System.Web'

$userParams = @{
   Name = 'ladmin'
   Description = 'WLAPS Client Admin'
   Password = [System.Web.Security.Membership]::GeneratePassword(16, 0) |
ConvertTo-SecureString -AsPlainText -Force
```

Run this script using the logged-on credentials: Yes [✓ No]

Enforce script signature check: Yes [✓ No]

Run script in 64-bit PowerShell: [✓ Yes] No

Migration

➔ It is possible to run legacy LAPS and Windows LAPS side-by-side if they target a distinct account. (Microsoft supported scenario)

Cleanup actions

- Unlink and delete old GPO’s
- Uninstall legacy LAPS agent (CSE component)
- Disable account which was managed by legacy LAPS
- Remove extended rights

Florian Salzmann

Cloud Consultant & MVP

@FlorianSLZ

Niklas Tinner

Endpoint Engineer

@NiklasTinner

Ask us in the Chat or reach out to us via our socials

Thank you

Read my blog post:
oceanleaf.ch/windows-laps-guide/

MODERN
ENDPOINT
MANAGEMENT
SERIES