Windows LAPS Adoption for ASC via Microsoft Intune and Azure AD

Strategy (Key Steps)

Steps: Why Move?   
Motivation Triggers

1. Migration:
   1. Cost Savings
   2. Reduction in Complexity
   3. Operation Optimization
   4. Increased business agility
   5. Customer Experience Improvements
2. Business Outcomes
   1. G
3. Business Justification (What’s my ROI)

Planning (Key Steps)

1. Digital Estate – Inventory of Assets
2. Initial Organization Alignment
3. Skills Readiness Plan
4. LAPS Adoption Plan

Ready (Key Steps)

1. LAPS Setup Guide
2. RBAC Setup Guide (Organize Roles and Responsibilities)

Adopt (Key Steps)

1. Deploy LAPS Policies to Target systems
2. Best Practices
3. Documentation & Hand off
4. Process improvements & Innovation

What is Windows LAPS:

Windows LAPS is the new built-in functionality in Windows that can be used for managing the password of a local administrator account on the device. Windows LAPS is the evolution of the already existing LAPS solution for domain joined Windows devices. Big difference, however, is that Windows LAPS policies can be now configured via Microsoft Intune and that can use Azure AD as a storage location for the local administrator password. Windows LAPS can be used to manage the password of a single local administrator account on the device.

Why Implement Windows LAPS:

The use of Windows LAPS helps organizations to further protect Windows devices from attacks that are aimed at exploiting local user accounts. Attacks like pass-the-hash or lateral-traversal. Besides that, Windows LAPS can also help with improving the security when providing remote support and with simply providing an alternative path for temporarily elevating permissions. Another common use case is providing an entrance to recover devices that became inaccessible for Azure AD accounts. And all of that by relying on native functionality that’s available on Windows devices with Windows 10 20H2 or later, and Windows 11 21H2 or later without the need for any 3rd party tools.

When using Microsoft Intune for the configuration of Windows LAPS, the configuration relies on the new [LAPS CSP](https://learn.microsoft.com/en-us/windows/client-management/mdm/LAPS-csp) on Windows devices. Via that CSP, Microsoft Intune provides support for the following capabilities of Windows LAPS:

* **Configuring password requirements**: Configuring password requirements for the local administrator account.
* **Configuring password rotation**: Configuring automatic password rotation on a schedule for the local administrator account and manually rotating the password for the local administrator account by using a device action.
* **Configuring account and password backup** – Configuring automatic account and password backup for the local administrator account in Azure AD, or Active Directory, by using strong encryption.
* **Configuring post authenticating actions** – Configuring the password expiration behavior (including how long the device waits) that a device takes when its local admin account password expires.
* **Viewing account details** – Viewing information about the local administrator account and its current password and see when that password was last rotated and when it’s next scheduled to rotate.
* **Viewing reports** – Viewing reports on password rotation with details about manual and scheduled password rotation.

Enabling Local Administrator Password Solution in Azure AD

To enable the usage of Windows LAPS in the Azure AD tenant.

1. Open [Microsoft Entra admin center](https://entra.microsoft.com/) navigate to **Azure Active Directory** >**Devices** > **Overview**> **Device settings.**
2. On the **Devices | Device settings** page, as shown below in Figure 1, switch the slider with **Enable Azure AD Local Administrator Password Solution (LAPS)**to **Yes**and click **Save.**

A screenshot of a computer

Description automatically generated

Steps to configure Windows LAPS and the options for retrieving, rotating and auditing the password of the local administrator account.

Configuring Windows Local admin password solution profile in Intune:

After enabling the LAPS functionality in Azure AD, the Windows devices must be configured to enable and configure Windows LAPS. That configuration can be achieved by using Microsoft Intune. More specifically, that configuration can be achieved by using an *Account protection* profile. When using Microsoft Intune for the configuration, it relies on the new [LAPS CSP](https://learn.microsoft.com/en-us/windows/client-management/mdm/LAPS-csp) in Windows. That CSP can handle the required configuration options. The following steps walk through the configuration of an *Account protection* profile that enables and configures Windows LAPS by using Azure AD as the storage location.

1. Open [Microsoft Intune admin center](https://intune.microsoft.com/) and navigate to **Endpoint security**>**Account protection**
2. On the **Endpoint security | Account protection** page, click **Create Policy**
3. On the **Create a profile** page, provide the following information and click **Create**

* **Platform**: Select **Windows 10 and later** as value
* **Profile**: Select **Local admin password solution (Windows LAPS)** as value

1. On the **Basics** page, specify a valid name to distinguish the policy from other similar policies and click **Next**
2. On the **Configuration settings** page, as shown below in Figure 1, provide at least the following information and click **Next**

* **Backup Directory**: Select **Backup the password to Azure AD only** to make sure that it’s stored in Azure AD
  + With **Password Age Days** switch the slider to *Yes* to enable password age and specify the age in days
* With **Administrator Account Name** switch the slider to *Yes* to enable the account name configuration and specify the account name of the managed local administrator account
* **Password Complexity**: Select **Large letters + small letters + numbers + special characters**, or one of the other less complex options, to add password complexity
* With **Password Length** switch the slider to *Yes* to enable password length and specify the password length
* **Post Authentication Actions**: Select **Reset the password and logoff the managed account**, or one of the other options, to configure the behavior upon expiration of the configured grace period
* With **Post Authentication Reset Delay** switch the slider to *Yes* to enable the password reset delay configuration and specify the reset delay in days.
* On the **Scope tags** page, configure the required scope tags and click **Next**
* On the **Assignments** page, configure the required assignment by selecting the applicable group and click **Next**
* On the **Create + Review** page, review the configuration and click **Create**

A screenshot of a computer

Description automatically generated

Note: The applied configuration is stored in the registry at *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Policies\LAPS*.

Verifying applied Local Administrator Password Solution configuration

After using Microsoft Intune for applying the configuration to a Windows device, Windows LAPS will be enabled and configured. The configuration is stored in the registry at HKLM\SOFTWARE\Microsoft\Policies\LAPS, as shown below in Figure 3 on the right. That registry key contains values for the different configuration options of Windows LAPS. Besides that, there is a new Event Log named LAPS available on the device, as shown below in Figure 3 on the left. That log contains all the events related to Windows LAPS. From the applied configuration, till any performed actions (like rotating the password).

A screenshot of a computer

Description automatically generated

Retrieving the password of the managed local administrator account

When Windows LAPS is enabled and configured for a device, the managed local administrator account and its password are stored in Azure AD and available via Microsoft Intune and Azure AD. That information is easily accessible for any IT administrator with the required permissions. Via Microsoft Intune, as shown below in Figure 4, the information is available via the **Local admin password** section of a device. After that, simply select **Show local administrator password** and click **Show** with *Local administrator password*, to retrieve the password of the managed local administrator account.

A screenshot of a computer

Description automatically generated

Rotating the password of the managed local administrator account

When using the password of the managed local administrator account, the configuration of Windows LAPS can make sure that the password will automatically rotate. Besides that, it’s also a relatively easy task for any IT administrator with the required permissions of: *Read* managed devices, *Read* organization, and *Rotate Local Admin Password* remote task. That task can be achieved in Microsoft Intune, as shown below in Figure 5, via the **Overview** section of a device. After that, simply select the three dots and click **Rotate local admin password**, to trigger the remote action to rotate the password of the selected device.

A screenshot of a computer

Description automatically generated

Auditing the managed local administrator account password activities

Besides all the configuration options and insights of Windows LAPS, there is also important audit information available. That provides any organization with the required information about the activities around the local administrator password on Windows devices. That information is easily accessible for any IT administrator, with the right permissions, and is available in the *Audit logs* in Azure AD, as shown below in Figure 6. The selected line is an example of a rotated password.

A screenshot of a computer

Description automatically generated