cloudcoffee.ch

Freshly brewed with Microsoft Azure and Microsoft 365

Windows LAPS in Microsoft Intune

BY OLIVER MÜLLER / ON 1. JULY 2023 / IN MICROSOFT 365

LAST UPDATED ON 15. OCTOBER 2024

Windows LAPS (Local Administrator Password Solution) provides centralized, simple, and secure management of local administrator passwords through Microsoft Intune. Each device receives its own, time-limited local administrator password. Windows LAPS independently manages the administrator passwords in terms of expiration and rotation. The passwords are stored either in Microsoft Entra ID (formerly Azure Active Directory) or in the local Active Directory.

The centralized management of all local administrator passwords simplifies control and monitoring. The time-controlled rotation of passwords significantly reduces their exposure duration. In addition, access to the stored passwords is strictly controlled, which makes unauthorized access more difficult and overall increases the security of the network environment.

This guide demonstrates how to configure Windows LAPS in Microsoft Intune to store local administrator passwords in Microsoft Entra ID.

Table of contents [hide]

Prerequisites and Licensing

Operating Systems

The following fully patched operating systems support Windows LAPS:

- **Windows 11**: Current supported version (recommended: Version 24H2, as it offers support for automatic administrator account management)
- **Windows 10**: Current supported version
- **Windows Server 2022**
- **Windows Server 2019**

Licensing

- Microsoft Entra ID Free or higher
  (when using administrative units Microsoft Entra ID P1 or higher)
- Microsoft Intune Plan 1 or higher

An overview of Microsoft 365 license packages with their features can be found at https://m365maps.com/.

Roles

A role with the **microsoft.directory/deviceLocalCredentials/password/read** permission is required to retrieve the local administrator password. This permission is part of the following roles:

- Global Administrator

- Intune Administrator
- Cloud Device Administrator

Enable Windows LAPS

The activation of Windows LAPS is done in the Microsoft Entra admin center (https://portal.azure.com).

Open **Identity > Devices** > **All devices > Device Settings** and enable the feature **Enable Microsoft Entra Local Administrator Password Solution (LAPS)**

Configure Windows LAPS

Create Intune policy

The policy for Windows LAPS is created in the Microsoft Intune admin center (https://intune.microsoft.com).

This guide leverages the features for automatic administrator account management and requires Windows 11 24H2. As these settings cannot be configured through the GUI at the time of writing, a configuration policy is used.

Open **Endpoint Security** > **Manage > Account protection** and create a new policy with **Create Policy**

Select Platform **Windows 10 and later (1)**, Profile **Templates (2)**, Template **Custom (3)** and create the policy with **Create (4)**.

Name the configuration policy (e.g., WCP_LAPS) and click Next.

Configuring Windows LAPS:

All policies are described in detail under LAPS-CSP | Microsoft Learn. The following Windows LAPS configuration serves as a suggestion and can be individually adapted and expanded.

Click **Add (1)** and set the following OMA-URI settings:

Name (2)	**OMA-URI (3)**	**Datentyp (4)**	**Wert (5)**
Directory the local admin account password is backed up to	./Device/Vendor/MSFT/LAPS/Policies/BackupDirectory	Integer	1
Maximum password age in days before the password is rotated	./Device/Vendor/MSFT/LAPS/Policies/PasswordAgeDays	Integer	30
Activate automatic account management	./Device/Vendor/MSFT/LAPS/Policies/AutomaticAccountManagementEnabled	Boolean	True
Activate automatically managed account	./Device/Vendor/MSFT/LAPS/Policies/AutomaticAccountManagementEnableAccount	Boolean	True
Set the name of the administrator account	./Device/Vendor/MSFT/LAPS/Policies/AutomaticAccountManagementNameOrPrefix	String	ccladmin
Append a random numerical suffix to the name of the administrator account for each rotation	./Device/Vendor/MSFT/LAPS/Policies/AutomaticAccountManagementRandomizeName	Boolean	True

Set account that is managed automatically	./Device/Vendor/MSFT/LAPS/Policies/AutomaticAccountManagementTarget	Integer	1
Set password complexity	./Device/Vendor/MSFT/LAPS/Policies/PasswordComplexity	Integer	7
Set password length	./Device/Vendor/MSFT/LAPS/Policies/PasswordLength	Integer	16
Select the action to be performed after authentication	./Device/Vendor/MSFT/LAPS/Policies/PostAuthenticationActions	Integer	3
Time period in hours until the selected action is executed	./Device/Vendor/MSFT/LAPS/Policies/PostAuthenticationResetDelay	Integer	24

1.

The assignment to devices can be customized here according to your specific needs.

Applicability rules can be created as needed.

The settings will be displayed for review once more, and the policy will be created by clicking **Create**.

The new policy for Windows LAPS is created immediately.

Retrieve Windows LAPS password

There are several ways to retrieve the local administrator password of a device. The procedure for Microsoft Entra admin center, Microsoft Azure Portal, and Microsoft Intune is described below.

Microsoft Entra

Sign in to Microsoft Entra admin center (https://entra.microsoft.com/).

Open **Identity > Devices** > **All devices** and select the device from which the local administrator password is to be displayed.

Under **Local administrator password recovery** > **Show local administrator password** the account name for the local administrator and the password are shown.

Microsoft Azure Portal

Sign in to Microsoft Azure Portal (https://portal.azure.com).

Open **Microsoft Entra ID > Manage > Devices** > **All devices** and select the device from which the local administrator password is to be displayed.

Under **Local administrator password recovery** > **Show local administrator password** the account name for the local administrator and the password are shown.

Microsoft Intune

Sign in to Microsoft Intune admin center (https://intune.microsoft.com).

Open **Devices > By platform > Windows**

Select the device from which the password for the local administrator is to be shown.

Under **Local admin password** > **Show local administrator password** the account name for the local administrator and the password are shown.

Who retrieved the local administrator password?

In the audit logs of Microsoft Entra, it can be clearly traced which User Principal Name had access to the local administrator password.

Open **Microsoft Entra Admin Center** (https://entra.microsoft.com) **> Identity > Monitoring & health** > **Audit logs**
Set filter:

- Service (1) = Device Registration Service
- Activity (2) = Recover device local administrator password
- Target (3) = corresponds to the hostname of the device. If the filter is not visible, it can be added through the **Add filter** option

Open log entry of the device

In the detailed audit log, the account that viewed the local administrator password is listed under the **User Principal Name** section.

Retrieve Windows LAPS password restricted to a group of devices

Administrative units can be used to granularly control access to Windows LAPS passwords. The Users with the role Cloud Device Administrator get access only to this administrative unit. This ensures that the user with Windows LAPS is only allowed to retrieve the passwords of devices that are assigned to this administrative unit. The use of administrative units requires an Microsoft Entra ID P1 license.

Create administrative unit

The administrative unit is created in Microsoft Entra admin center or the Azure Portal. This guide uses the Microsoft Entra admin center (https://entra.microsoft.com).

Create the administrative unit with **Identity > Roles & admins** > **Admin units** > **Add**.

Enter a name for the administrative unit.

Assign all users to the Cloud Device Administrator role who are allowed to retrieve the Windows LAPS passwords of the devices of this administrative unit.

Click on **Create** to create the administrative unit.

The administrative unit has been created.

Assign devices to a administrative unit

Open the administrative unit in **Microsoft Entra Admin Center** (https://entra.microsoft.com) **> Identity > Roles & admins** > **Admin units**

Click on **Devices** > **Add devices**

Assign devices to the administrative unit.

Users with the Cloud Device Administrator role on this administrative unit are allowed to retrieve the Windows LAPS passwords of all listed devices.

Local administrator password recovery is shown for authorized devices.

Local administrator password recovery is not shown for unauthorized devices.

Retrieve Windows LAPS password history

PowerShell allows to read the password history of the local administrator account. This can be useful if a device is restored to a previous restore point and thus the current local administrator password is not valid. With PowerShell, a maximum of the last three local administrator passwords are displayed.

To be able to retrieve the Windows LAPS password history, the PowerShell cmdlet **Microsoft.Graph** is required.

```
Install-Module microsoft.graph -Scope AllUsers
```

Connect to Microsoft Graph and set the two permissions **Device.Read.All** and **DeviceLocalCredential.Read.All**.

```
Connect-MgGraph -Scope "Device.Read.All","DeviceLocalCredential.Read.All"
```

The **Get-LapsAADPassword** cmdlet displays the last three local administrator passwords.

Replace parameter **-DeviceIDs** with the device name.

```PowerShell
Get-LapsAADPassword -DeviceIds OMUVWSWX001 -IncludePasswords -AsPlainText -IncludeHist
```

The output shows the last three local administrator passwords (1-3) in plain text with the respective expiration date.

Rotate Windows LAPS password

Windows LAPS automatically rotates the password according to settings in the policies. If the password needs to be rotated before the maximum password age is reached, this must be done manually in the Microsoft Intune admin center (https://intune.microsoft.com).

Open **Devices > By platform > Windows**

Select the device on which the password for the local administrator is to be rotated.

In the **Overview**, click on the three dots and select **Rotate local admin password**.

Confirm the message with **Yes**. At the next restart Windows LAPS rotates the password on this device.

Troubleshooting

Windows LAPS stores the activities in the following logs.

Audit logs in Microsoft Intune

All activities of Windows LAPS are stored in the audit logs of the Microsoft Intune admin center (https://intune.microsoft.com).

Open **Tenant administration** > **Audit logs**

Set the filter **Category (1)** to **Device** and select the **date range (2)**.

Select the activity for details.

Event viewer on device

Windows LAPS activities are stored in the Event Viewer of the device.

Open **Event Viewer** > **Application and Services Logs** > **Microsoft** > **Windows** > **LAPS** to track the activities.

Follow me on LinkedIn to always stay updated on my recent posts.

Follow on LinkedIn

Was this post helpful to you? Show your enthusiasm with the delightful aroma of a freshly brewed coffee for me!

MICROSOFT ENTRA MICROSOFT INTUNE MICROSOFT TENANT HARDENING POWERSHELL TROUBLESHOOTING

PREVIOUS

Show First Contact Safety Tip in Email

NEXT

Seamless Upgrade of Windows Server on Azure: Best Practices and Step-by-Step Guide