

Tech Community Live: Microsoft Security

Dec 03 2024, 07:00 AM - 11:30 AM (PST) 📍 Microsoft Tech Community

Find out more >

[Home](#) > [Security, Compliance, and Identity](#) > [Microsoft Entra Blog](#)
> [Introducing Windows Local Administrator Password Solution with Microsoft Entra \(Azure AD\)](#)

Back to Blog

< Newer Article

Older Article >

Introducing Windows Local Administrator Password Solution with Microsoft Entra (Azure AD)

By  [Alex Simons \(ENTRA\)](#)

Published Apr 21 2023 09:00 AM

🔊 83.6K Views



Howdy folks,

Today we have some news I know many of you will be excited about! As part of our vision to give you comprehensive security solutions, we’ve joined forces with the Windows and Microsoft Intune teams to release a **public preview** of **Windows Local Administrator Password Solution (LAPS) for Azure AD** (which is now part of Microsoft Entra).

I’ve asked Sandeep Deo, one of the Product Managers behind this release, to give you the low down on all these updates and explain how you can start using Windows LAPS with Microsoft Entra (Azure AD). You’ll find Sandeep’s blog post below.

Best regards,

Alex Simons (@Alex_A_Simons)
Corporate VP of Program Management
Microsoft Identity Division

Hi everyone,

I am excited to share with you the updates we have made to LAPS and how you can start using it with Microsoft Entra (Azure AD) and Microsoft Intune to secure your Windows devices joined to Azure AD.

Every Windows device has a built-in local administrator account that you must secure and protect to mitigate any Pass-the-Hash (PtH) and lateral traversal attacks. Many customers have been using our standalone, on-premises LAPS product for local administrator password management of their domain-joined Windows machines. We heard from many of you that you need LAPS support as you modernize your Windows environment to join directly to Azure AD.

Today we're making Windows LAPS available to you for both Azure AD joined and hybrid Azure AD joined devices. Additionally, Windows LAPS is now built-in into Windows with

Co-Authors



[Alex Simons \(AZURE\)](#)

Version history

Last update: Apr 24 2023 08:52 AM
Updated by: [SHDriggers](#)

Labels

Product Announcements

257

Share



later using the most recent security update (released on April 11, 2023). With these updates, you wi...

There are some pretty important capabilities we've enabled within this preview:

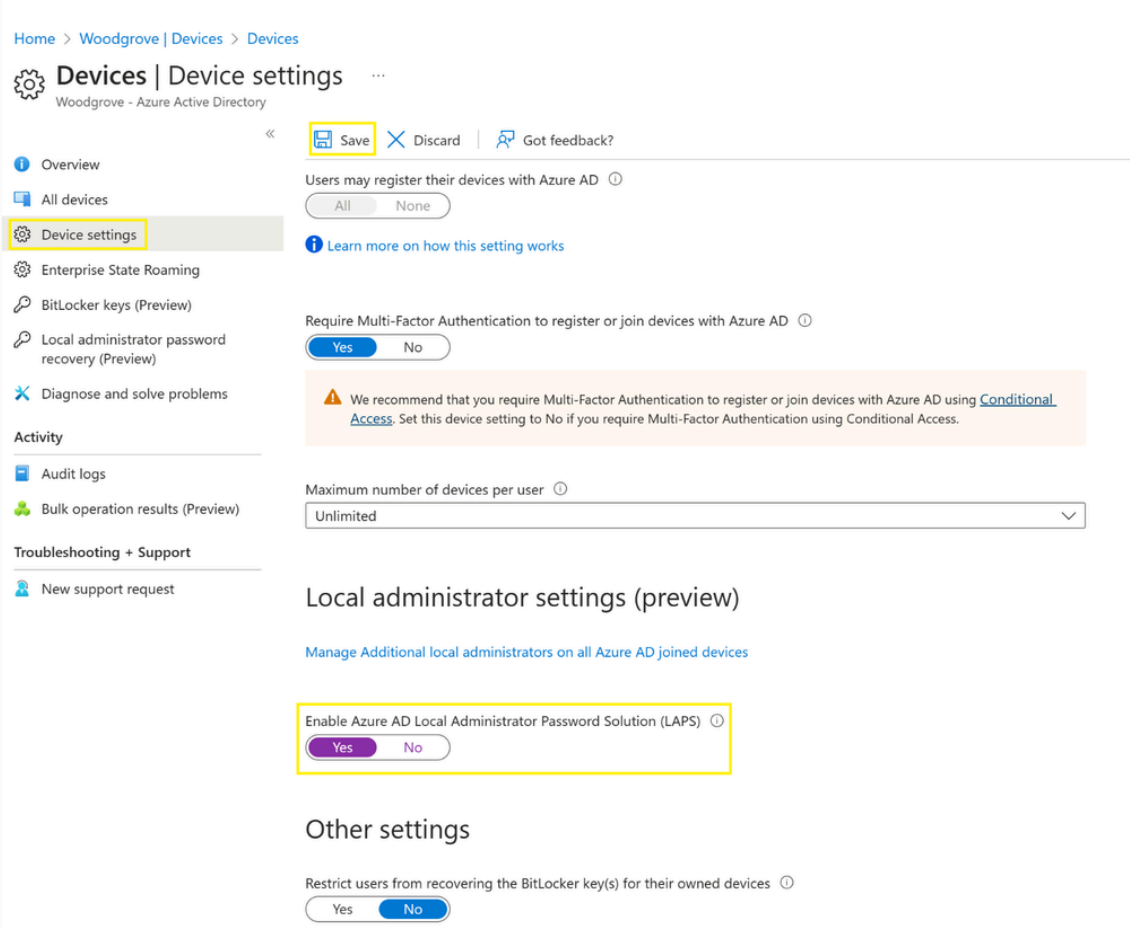
- Turn on Windows LAPS using a **tenant-wide policy and a client-side policy to backup local administrator password to Azure AD.**
- Configure **client-side policies via Microsoft Intune portal for local administrator password management to set account name, password age, length, complexity, manual password reset and so on.**
- Recover **stored passwords via Microsoft Entra/Microsoft Intune portal or Microsoft Graph API/PSH**
- Enumerate all LAPS-enabled devices via **Microsoft Entra portal or Microsoft Graph API/PSH.**
- Create **Azure AD role-based access control (RBAC) policies with custom roles and administrative units for authorization of password recovery.**
- View **audit logs via Microsoft Entra portal or Microsoft Graph API/PSH to monitor password update and retrieval events.**

Configure **Conditional Access policies on directory roles that have the authorization of password recovery.**

Let’s walk through the simple steps to enable some of these scenarios.

Setting up LAPS

In the **Azure AD Devices** menu, select **Device settings**, and then select **Yes** for the **LAPS setting** and click **Save**.



In the **Microsoft Intune Endpoint security** menu, select **Account protection**, then select **Create Policy** to create a Windows LAPS profile for Windows 10 and later. During profile creation, the pick **Backup Directory to be Azure AD** and can also configure other client policies for LAPS, does the **Assignments** to Azure AD groups and then finally selects **Review + Create**.

Home > Endpoint security

Endpoint security | Account protection

Search

Create PolicyRefreshExport

Overview

Overview

All devices

Security baselines

Security tasks

Manage

Antivirus

Disk encryption

Firewall

Endpoint Privilege Management

Endpoint detection and response

Attack surface reduction

Account protection

Device compliance

Conditional access

Monitor

Assignment failures

Setup

Microsoft Defender for Endpoint

Help and support

Help and support

Search by profile name

Policy name	Policy type	Assigned
No results		

Create a profile

Platform

Windows 10 and later

Profile

Local admin password solution (Windows LAPS) (preview)

Local admin password solution (Windows LAPS) (preview)

Windows Local Administrator Password Solution(Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on your Azure Active Directory - joined or Windows Server Active Directory - joined devices.

Create

Home > Endpoint security | Account protection >

Create profile

Local admin password solution (Windows LAPS) (preview)

1 Basics

2 Configuration settings

3 Scope tags

4 Assignments

5 Review + create

Name *

WindowsLAPS

Description

Deploy LAPS policy to Windows

Platform

Windows 10 and later

PreviousNext

[Skip to Primary Navigation](#)

Page 3 of 12

Home > Endpoint security | Account protection >

Create profile ...

Local admin password solution (Windows LAPS) (preview)

- ✓ Basics
- 2 Configuration settings**
- 3 Scope tags
- 4 Assignments
- 5 Review + create

^ LAPS

Backup Directory ⓘ

Backup the password to Azure AD only

▼

Password Age Days ⓘ

Not configured

30

Administrator Account Name ⓘ

Not configured

Password Complexity ⓘ

Not configured ▼

Password Length ⓘ

Not configured

Post Authentication Actions ⓘ

Not configured ▼

Post Authentication Reset Delay ⓘ

Not configured

Previous

Next

Recovering local administrator password

In the **Azure AD Devices | Overview page**, select **Local admin password recovery** option. This will enumerate all devices that are enabled with LAPS and then click **Show local administrator password** next to the device name to recover the password. You will also have the option to enter device name to filter from the enumerated list and then choose **Show local administrator password**.

Home > Woodgrove | Devices > Devices

Devices | Local administrator password recovery (Preview) ...

Woodgrove - Azure Active Directory

Overview

All devices

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Local administrator password recovery (Preview)

Diagnose and solve problems

Refresh

Got feedback?

Search by device name

Add filters

2 local admin passwords found

Device name	Local administrator password	Last password rotation
Win11LAPSAADI	Show local administrator password	4/13/2023, 12:58:24 PM
MSCOTT-SURFACE2	Show local administrator password	4/13/2023, 1:09:50 PM

Local administrator password

Account name

sandeo

Security ID

S-1-5-21-2013787640-181955172-240414245-500

Local administrator password

***** Show

Last password rotation

4/13/2023, 12:58:24 PM

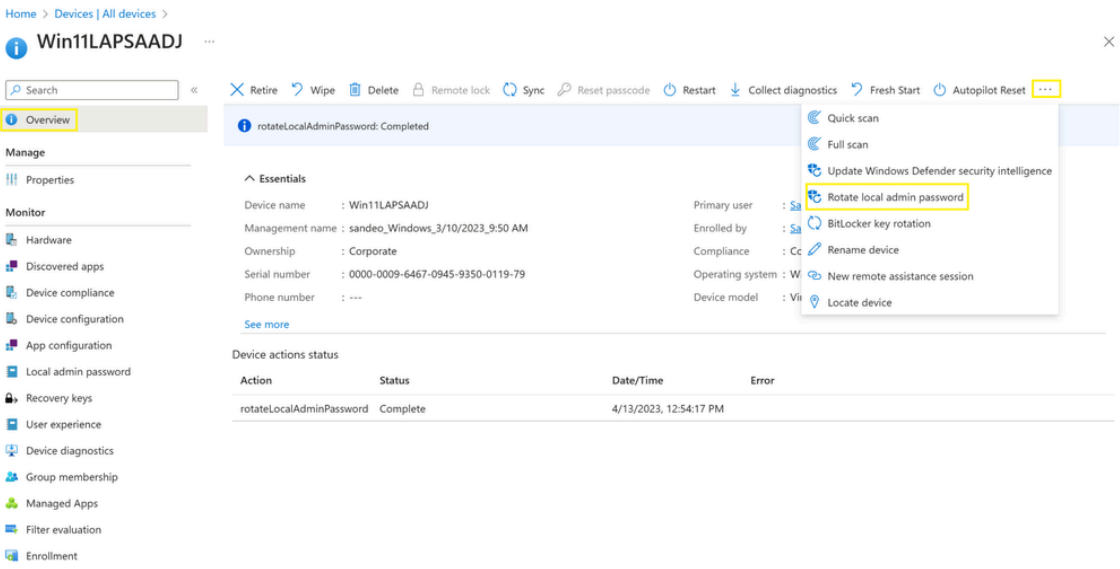
Next password rotation

5/13/2023, 12:58:23 PM

You can also create [custom roles](#) or [administrative units](#) in Azure AD for authorization of local administrator password recovery.

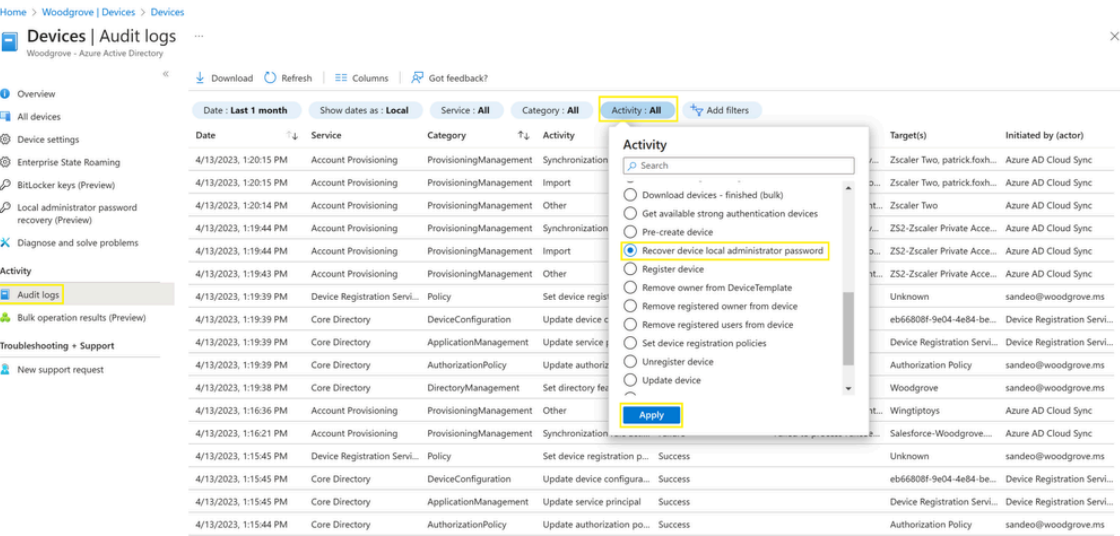
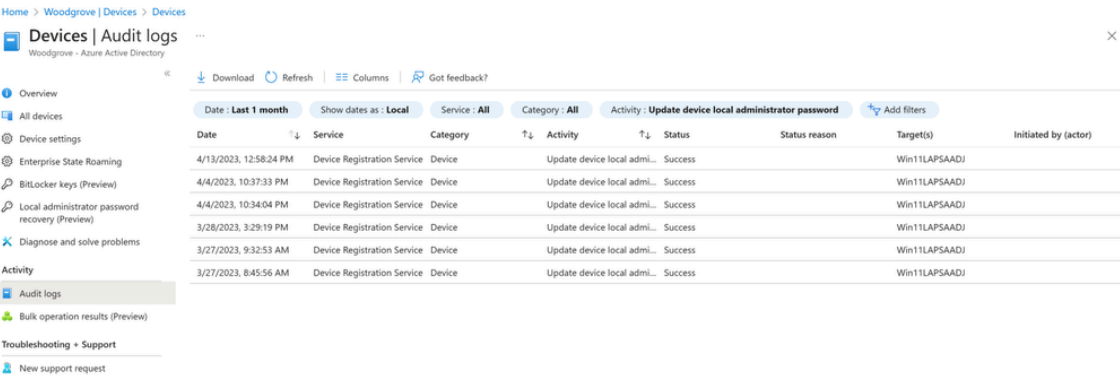
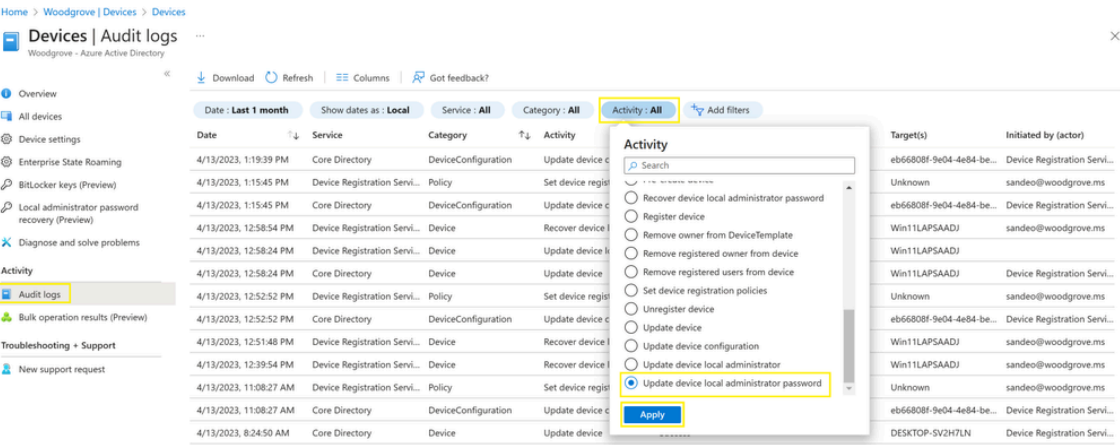
Reset local administrator password manually

In the **Microsoft Intune Endpoint Devices | All devices** page, enter the device name in the **Search** field. Then on the specific device’s overview page choose the device action **Rotate local admin password**.



Audit local administrator password update and recovery

In the **Azure AD Devices | Overview** page, pick **Audit logs**, then use **Activity** filter and **Search** for **Update device local administrator password** or **Recover device local administrator password** to view the audit events.



Home > Woodgrove > Devices > Devices

Devices | Audit logs

Woodgrove - Azure Active Directory

Download Refresh Columns Got feedback?

Overview

All devices

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Local administrator password recovery (Preview)

Diagnose and solve problems

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Date: Last 1 month

Show dates as: Local

Service: All

Category: All

Activity: Recover device local administrator password

Add filters

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
4/13/2023, 12:58:54 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/13/2023, 12:51:48 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/13/2023, 12:39:54 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/13/2023, 12:33:06 AM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/13/2023, 12:31:40 AM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/7/2023, 3:12:51 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/7/2023, 3:10:58 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/7/2023, 3:10:13 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/7/2023, 2:34:09 PM	Device Registration Servi...	Device	Recover device local ad...	Success		MSCOTT-SURFACE2	sandeo@woodgrove.ms
4/5/2023, 4:13:01 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/4/2023, 10:35:50 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/4/2023, 10:31:05 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/4/2023, 10:21:43 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms
4/4/2023, 10:21:13 PM	Device Registration Servi...	Device	Recover device local ad...	Success		Win11LAPSAADJ	sandeo@woodgrove.ms

You can click on the individual audit events to get more details like activity, target(s), and modified properties.

We strongly recommend you deploy Windows LAPS with Microsoft Entra (Azure AD) and Microsoft Intune to take advantage of the new security improvements. Doing this will be much more secure for these sensitive passwords. To get started with Windows LAPS for Microsoft Entra (Azure AD), go [here](#).

As always, we'd love to hear your feedback, thoughts, and suggestions! Feel free to share with us on the [Microsoft Entra \(Azure AD\) forum](#) or leave comments below. We look forward to hearing from you.


Best regards,
Sandeep Deo (@MsftSandeep)
Principal Product Manager
Microsoft Identity Division

Learn more about Microsoft identity:

- Related Articles: [Microsoft Intune support for Windows LAPS](#), [Windows LAPS technical documentation](#), [Windows LAPS CSP reference](#)
- Get to know [Microsoft Entra](#) – a comprehensive identity and access product family
- Return to the [Microsoft Entra \(Azure AD\) blog home](#)
- Join the conversation on [Twitter](#) and [LinkedIn](#)
- Share product suggestions on the [Microsoft Entra \(Azure AD\) forum](#)

4 Likes

22 Comments




[Seth Kusiak](#) Copper Contributor

Apr 21 2023 10:19 AM

is there an additional cost to using this new capability?

0 Likes



[Zack_269](#) Copper Contributor

Apr 21 2023 11:54 AM

Is there a significant delay between enabling LAPS within Device settings and being able to create a profile? I enabled the Azure AD LAPS setting around 15 minutes ago, and still only see Local user group membership and Account protection (Preview) within the profile types when creating an Account protection profile for Windows 10 and later.

I have refreshed, logged out/in, tried a different browser.

Thanks for bringing this functionality to Intune!

👍 1 Like



[CristopherAlaya](#) Iron Contributor



Apr 21 2023 12:00 PM

[@Zack_269](#)

You probably have to wait for your tenant to be upgrade to Intune release 2304.

<https://techcommunity.microsoft.com/t5/microsoft-intune-blog/what-s-new-in-microsoft-intune-2304-apr...>

My tenant usually updates late in the weekend after the new features are announced.

👍 0 Likes



[Zack_269](#) Copper Contributor



Apr 21 2023 12:03 PM

[@CristopherAlaya](#) I was just coming back to post that. I see we're on 2303 still, and as we're in NA, it'll be a couple of days. Will check back in on Monday. Thanks.

👍 1 Like



[CristopherAlaya](#) Iron Contributor



Apr 21 2023 12:54 PM

[@Seth Kusiak](#)

<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-manage-local-admin-passwords#...>

👍 0 Likes



[LewisBarryMVP](#) Iron Contributor



Apr 21 2023 01:43 PM

Please evaluate and understand the impact of deploying this solution. Think about whether you really need it or not, as local admin rights are no small deal.

👍 0 Likes



[ylaskin](#) Copper Contributor



Apr 23 2023 04:56 AM

I don't see "**Enable Azure AD Local Administrator Password Solution (LAPS) in my tenant, any idea why?**

0 Likes



[Andrew King](#) Copper Contributor



Apr 23 2023 09:32 AM

Is there a roadmap for migrations from the on-premise LAPS to this new version of LAPS? The related question, we use LAPS today, is there an advisory of how to pilot this release in an environment that already has LAPS? IE should we exclude pilot systems from the current LAPS policies and uninstall the stand-alone LAPS client if we deployed it - so there is not a conflict between Intune policies and Group Policies?

0 Likes



[Paul Bendall](#) Iron Contributor



Apr 24 2023 05:24 AM

An excellent feature which will really help reduce lateral movement.

Can someone confirm that setting "**Enable Azure AD Local Administrator Password Solution (LAPS)**" by itself doesn't change the local admin password for existing devices? In effect, it just gives the ability to create a Profile in Intune?

I want to pilot new LAPS and create associated documentation with a small number of machines using a specific AU for the scope. My assumption is I need to enable LAPS using the above setting and then target the AU with the Profile in Intune, but this won't effect any existing machine that isn't in the AU

Thanks,

Paul

2 Likes



[CloudM1](#) Copper Contributor



Apr 24 2023 12:35 PM

Why do I want to enable or rely on LAPS when a modern Windows 11 device signed to Azure AD and manage with INTUNE has local Administrator account disabled?

1 Like

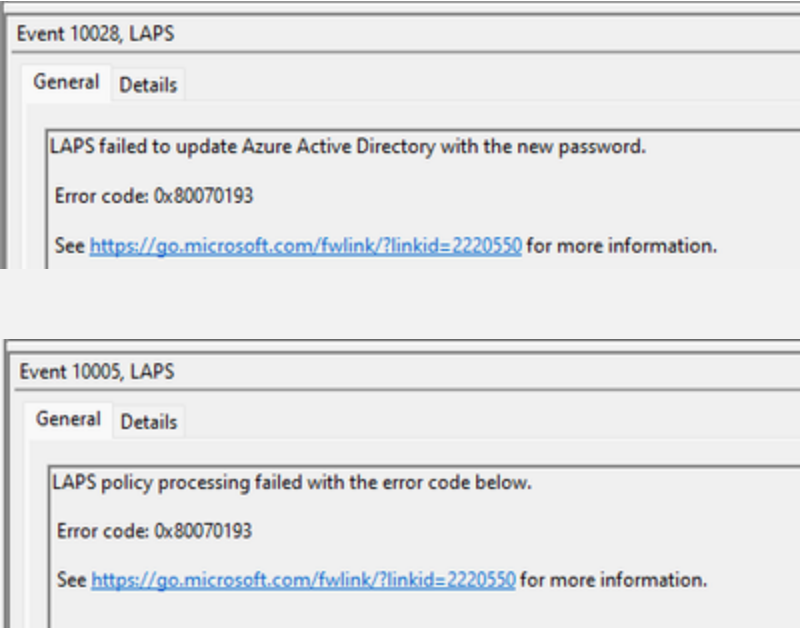


[Brian Hitner](#) Copper Contributor

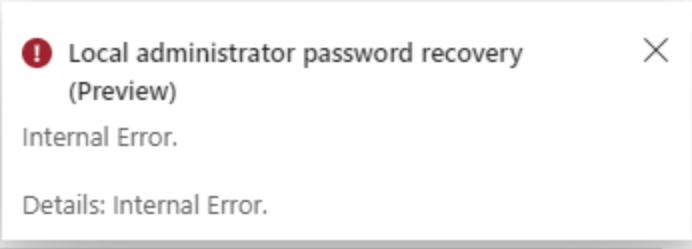


Apr 24 2023 10:17 PM

I have enabled LAPS Preview from Intune and I see in the eventvwr logs that the policy has successfully pushed down to the device, but fails to upload a new password to the tenant:



When I click on the *Local admin Password* tab in the Intune portal, I get this error



Additionally, there is no option in the Azure portal to "Enable Azure AD Local Administrator Password Solution (LAPS)", although some documentation has mentioned that once in public preview that should not be needed.

Is this a "Preview" bug?

Thanks

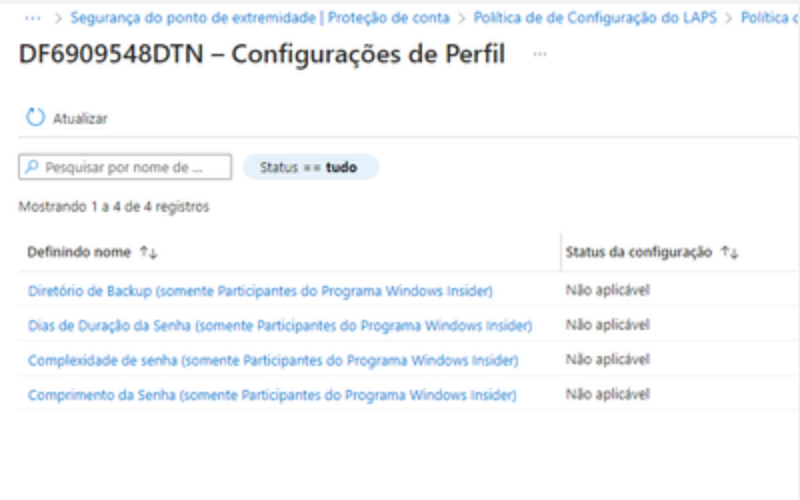
0 Likes



[Lucioj78](#) Copper Contributor

Apr 25 2023 01:13 PM

Is it only available for Windows Insiders Program members? 😞



0 Likes



[bkirk](#) Copper Contributor

Apr 26 2023 04:41 AM

Will now look into how to do it on our servers 😊

👍 0 Likes



[Brian Hitner](#) Copper Contributor

...

Apr 26 2023 08:05 AM

All working for me now.
It was just a matter of waiting for the preview features to fully upload to Azure.
I turned on the feature in Azure to "Enable Azure AD Local Administrator Password Solution (LAPS)" and within minutes the policy had populated correctly to my test group with a predefined custom admin user.

👍 0 Likes



[Hypnotix](#) Copper Contributor

...

May 02 2023 09:23 AM

Is there documentation on how to use GPO instead of Intune?
Our devices are hybrid joined to AAD, but they are not in Intune, as we are not ready to use it yet.

👍 0 Likes



[Quinn Wade](#) Brass Contributor

...

May 03 2023 05:02 PM

[@Hypnotix](#) I just did this today. Our devices our HAADJ. We're not using Intune to manage our devices either at this time. Still testing. So SCCM is our primary. I used these links to setup our migration from Legacy to Windows LAPS. The 2nd link from The Lazy Administrator was really helpful with creating the App Registration

[Get started with Windows LAPS and Azure Active Directory | Microsoft Learn](#)

[Windows LAPS Management, Configuration and Troubleshooting Using Microsoft Intune – The Lazy Adminis...](#)

👍 0 Likes



[SwapnilKadia](#) Copper Contributor

...

May 07 2023 08:27 PM

We currently have Legacy LAPS deployed to Hybrid Azure-AD devices via on-prem AD GPO. If we switch to Windows LAPS can we run Legacy LAPS and Windows LAPS side by side for **same local administrator account?**

With the Legacy LAPS and Windows LAPS running side by side, can Windows LAPS take priority and manage passwords for local administrator account without issues?

Is there a step-by-step guide available to switch from Legacy LAPS to Windows LAPS where we using same local administrator account?

0 Likes



[sg328](#) Copper Contributor



May 24 2023 03:26 AM

As per Pauls question:

Can someone confirm that setting "**Enable Azure AD Local Administrator Password Solution (LAPS)**" by itself doesn't affect existing devices? In effect, it just gives the ability to create a Profile in Intune?

Thanks

0 Likes



[Hrishikesh719](#) Copper Contributor



Sep 11 2023 10:03 AM

Hi @MsftSandeep ,
Does it work on Workgroup machine ? We have few meeting rooms which are not in Domain. They are all Teams PRO licensed.

0 Likes



[BobPendon](#) Copper Contributor



Dec 12 2023 05:17 PM

What will happen when I enable LAPS without configuring a policy?

0 Likes



[Michael54](#) Copper Contributor



Mar 04 2024 07:55 AM

since policies in Endpoint Manager can only be applied to workstations, does this mean you cannot use LAPS for server OS's?

0 Likes



[mpoulton](#) Copper Contributor



Apr 19 2024 12:48 PM

Does this LAPs solution work for vpn users?

👍 0 Likes

You must be a registered user to add a comment. If you've already registered, sign in. Otherwise, register and sign in.

[Comment](#)

What's new

- Surface Pro 9
- Surface Laptop 5
- Surface Studio 2+
- Surface Laptop Go 2
- Surface Laptop Studio
- Surface Duo 2
- Microsoft 365
- Windows 11 apps

Business

- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft Industry
- Small Business

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Virtual workshops and training
- Microsoft Store Promise
- Flexible Payments

Developer & IT

- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- Education consultation appointment
- Educator training and development
- Deals for students and parents
- Azure for students

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability



Your Privacy Choices

Sitemap

Contact Microsoft

Privacy

Manage cookies

Terms of use

Trademarks

Safety & eco

About our ads

© Microsoft 2024