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

By Alex Simons (ENTRA)

Published Apr 21 2023 09:00 AM 83.5K 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).

Skip to Primary Navigation

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 Windows 10 20H2 and later, Windows 11 21H2 and later, and Windows Server 2019 and 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.**

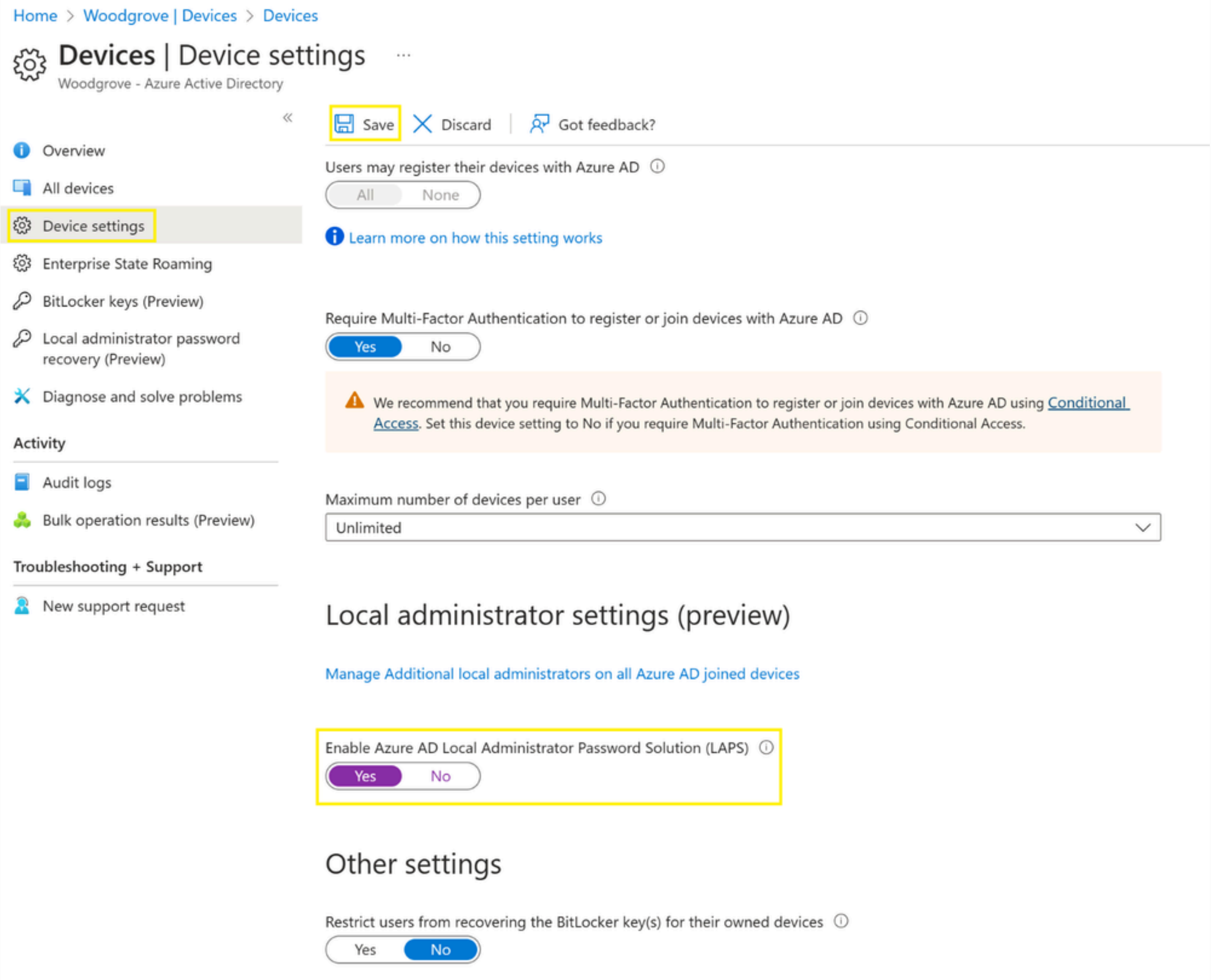
Skip to Primary Navigation

- 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.**



Home > Woodgrove | Devices > Devices

Devices | Device settings ...

Woodgrove - Azure Active Directory

Save Discard 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

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

⚠ We recommend that you require Multi-Factor Authentication to register or join devices with Azure AD using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ⓘ
Unlimited

Local administrator settings (preview)

Manage Additional local administrators on all Azure AD joined devices

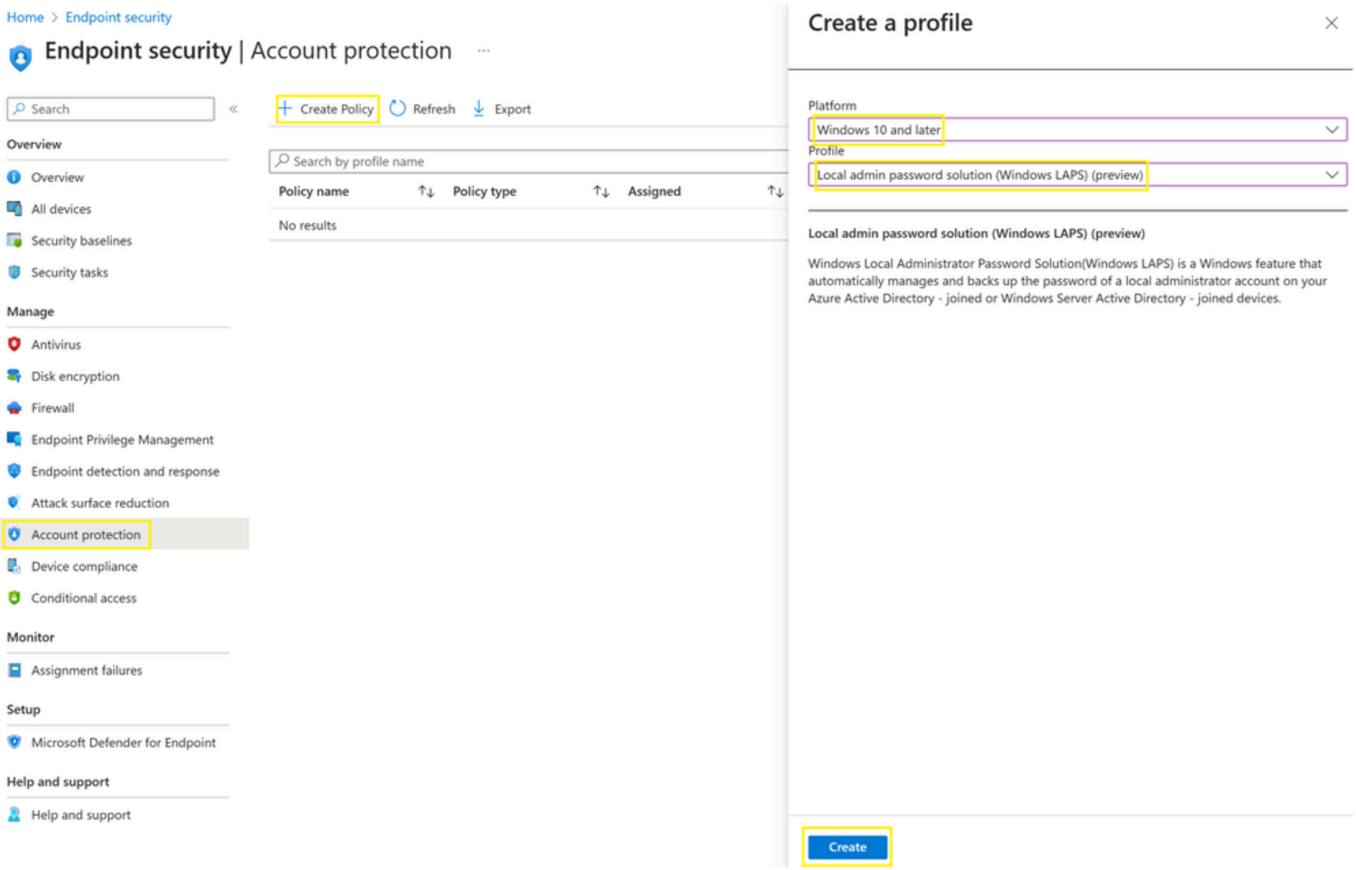
Enable Azure AD Local Administrator Password Solution (LAPS) ⓘ
[✓ Yes] No

Other settings

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

In the **Microsoft Intune Endpoint security** menu, select **Account protection**, then select**Create Policy** 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.**

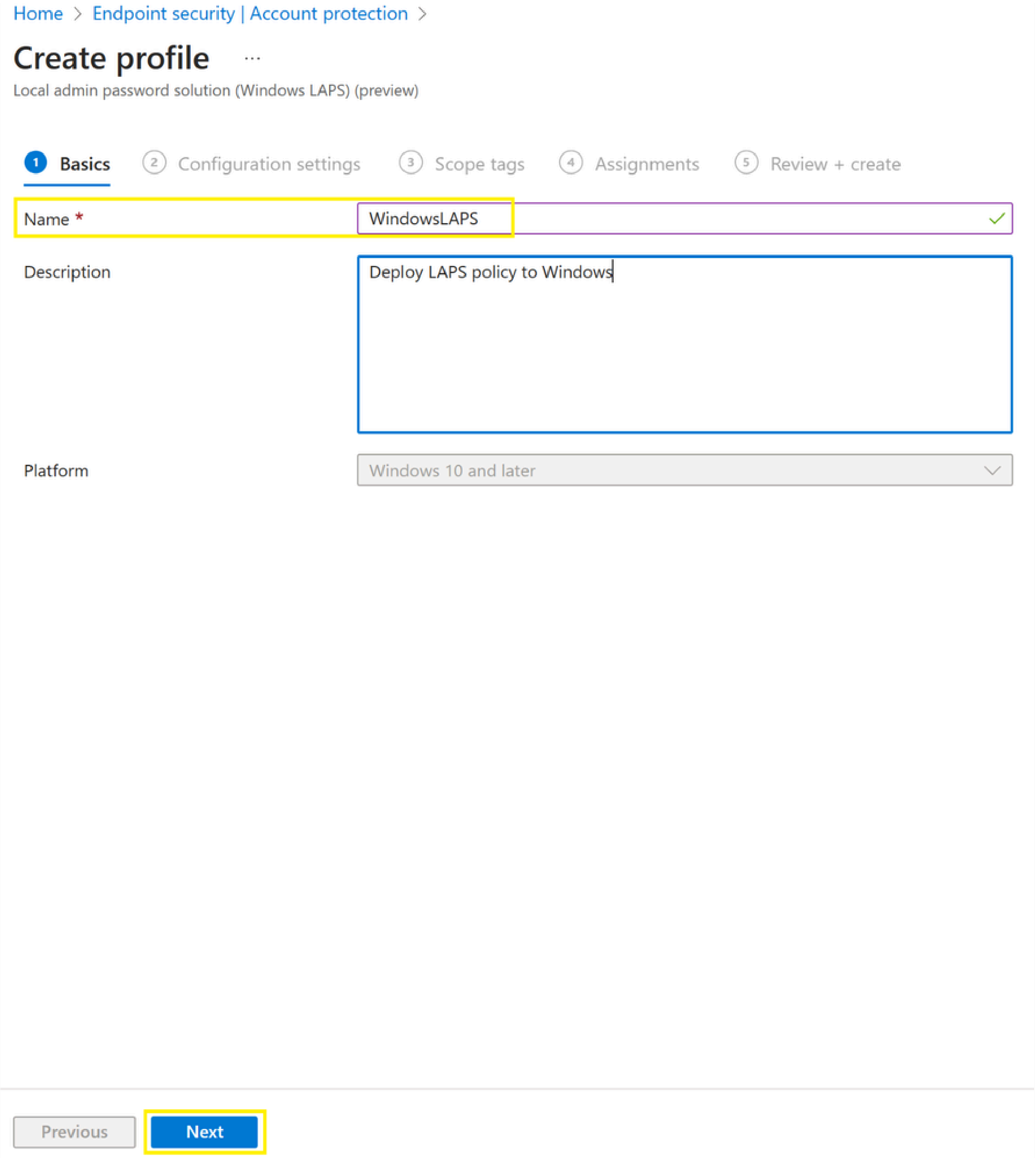


Platform: Windows 10 and later

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.

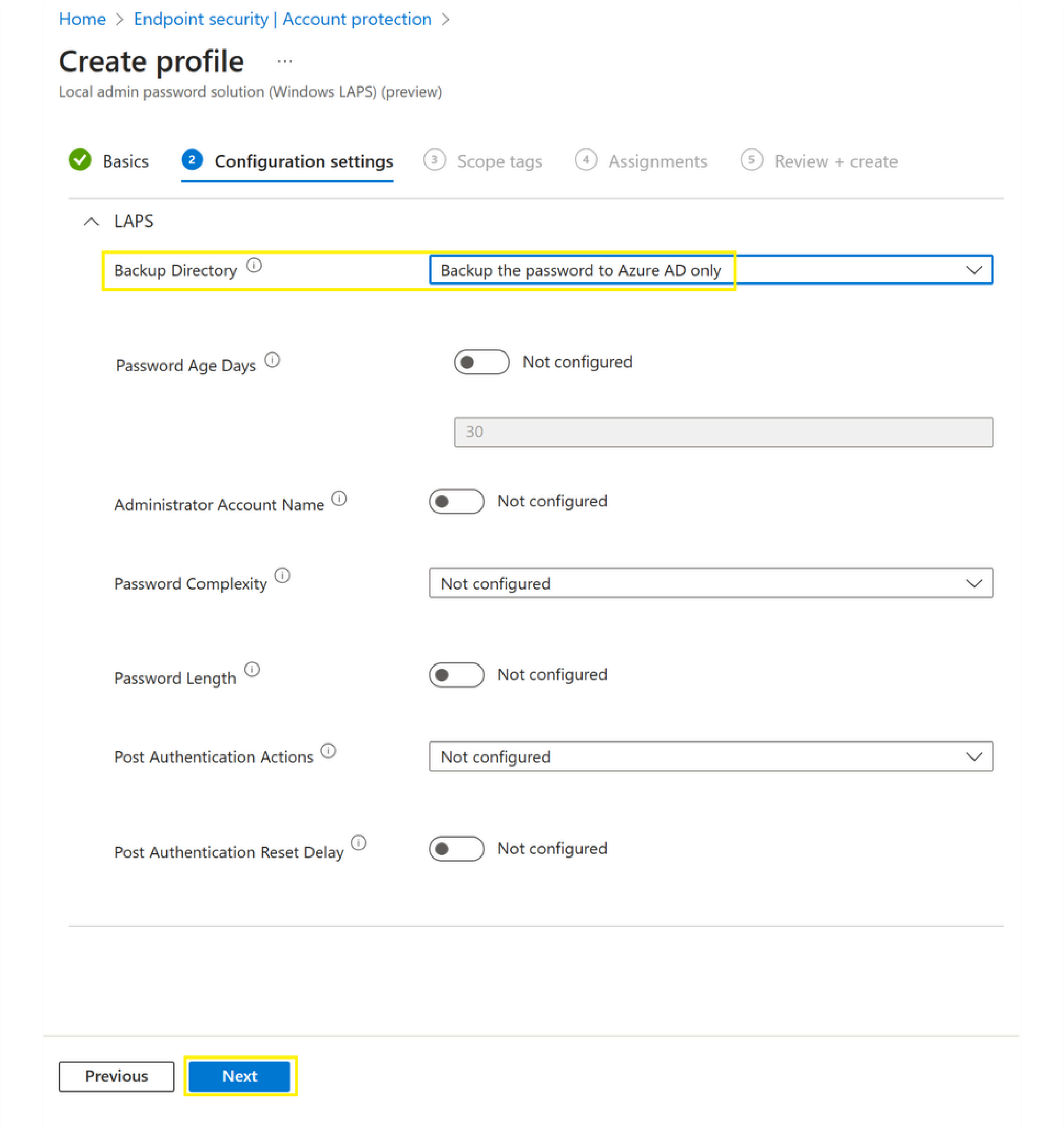


Name * WindowsLAPS ✓

Description Deploy LAPS policy to Windows

Platform Windows 10 and later

Skip to Primary Navigation



Home > Endpoint security | Account protection >

Create profile ...

Local admin password solution (Windows LAPS) (preview)

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

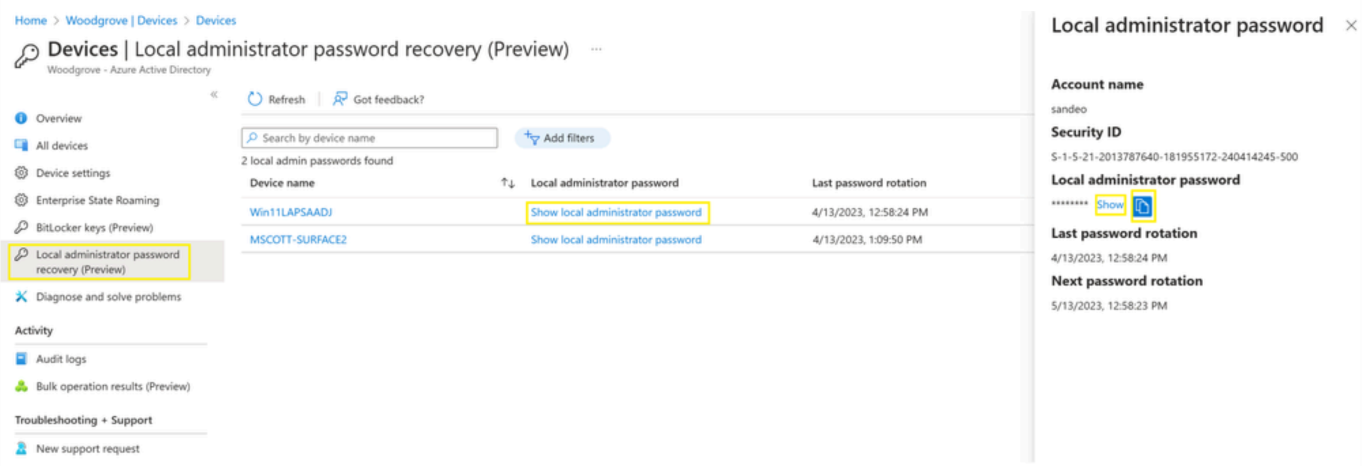
Password Length: Not configured

Post Authentication Actions: Not configured

Post Authentication Reset Delay: Not configured

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


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
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Refresh
Got feedback?
Search by device name
Add filters
Local administrator password
Show

2 local admin passwords found

Device name	Local administrator password	Last password rotation
Win11LAPSAADJ	Show local administrator password	4/13/2023, 12:58:24 PM
MSCOTT-SURFACE2	Show local administrator password	4/13/2023, 1:09:50 PM

Account name
sandeo

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

Local administrator password
****

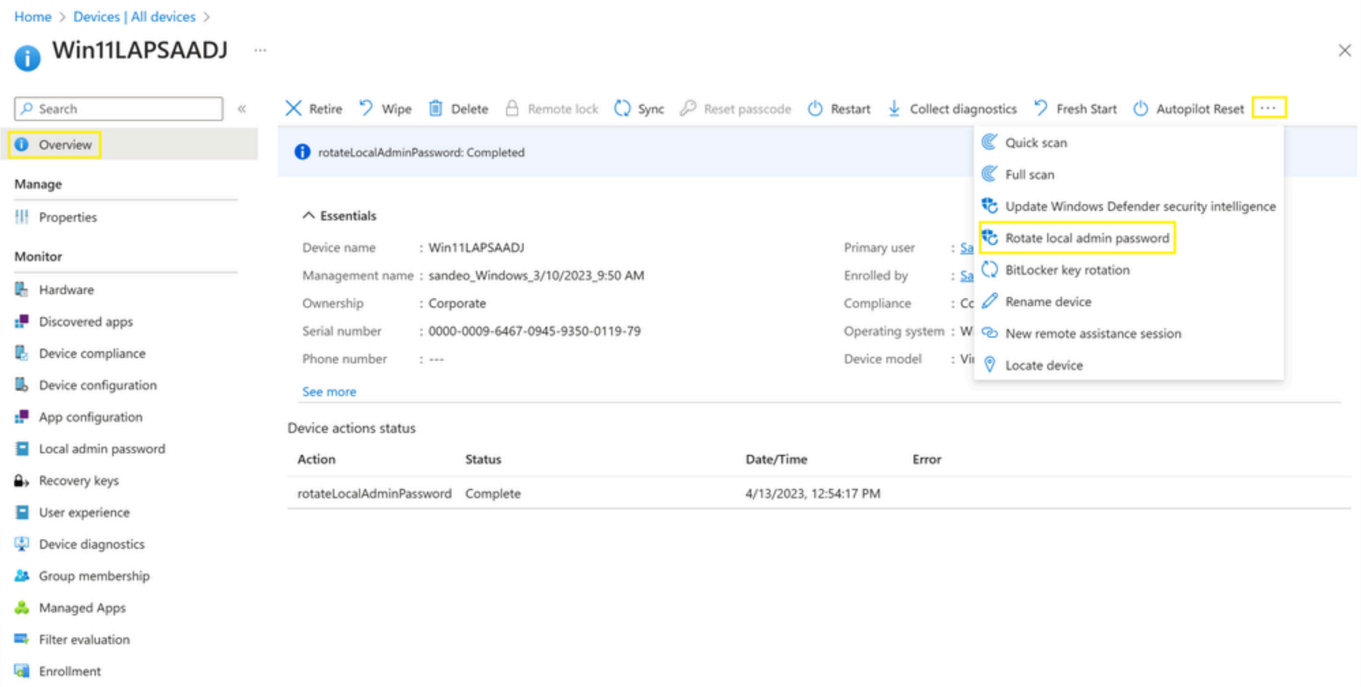
Last password rotation
4/13/2023, 12:58:24 PM

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**.



rotateLocalAdminPassword: Completed

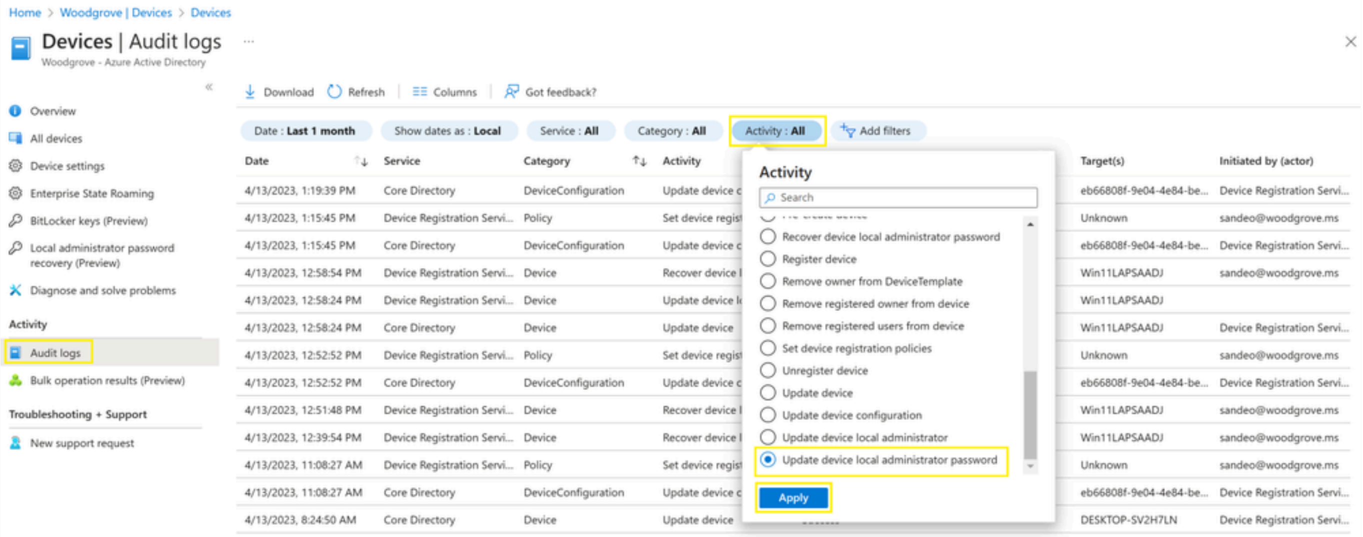
Device name : Win11LAPSAADJ
Management name : sandeo_Windows_3/10/2023_9:50 AM
Ownership : Corporate
Serial number : 0000-0009-6467-0945-9350-0119-79
Phone number : ---
Primary user : Sa
Enrolled by : Sa
Compliance : Co
Operating system : W
Device model : Vi

Device actions status

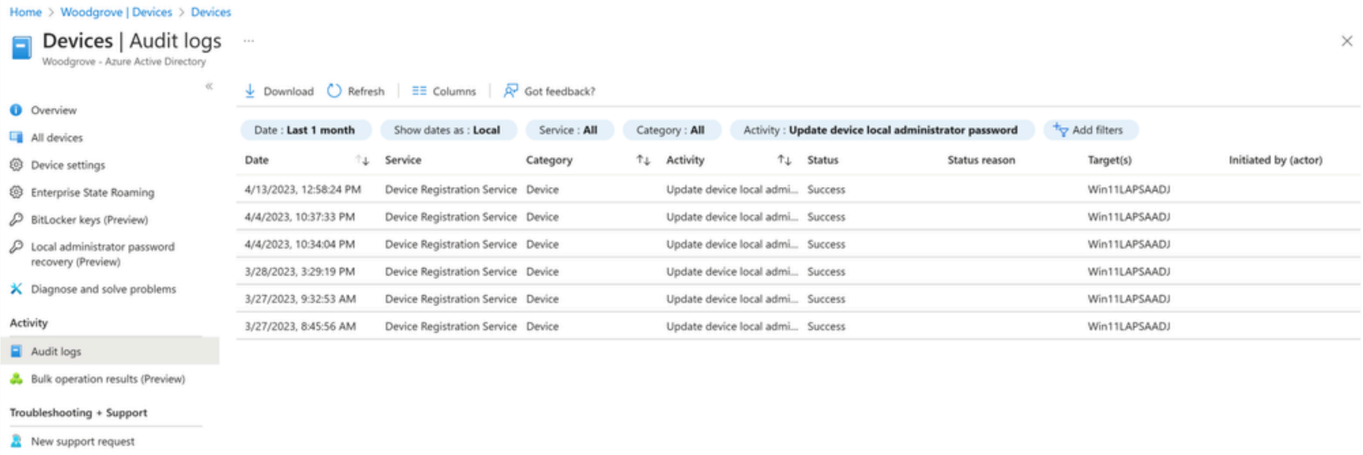
Action	Status	Date/Time	Error
rotateLocalAdminPassword	Complete	4/13/2023, 12:54:17 PM	

Audit local administrator password update and recovery

events.

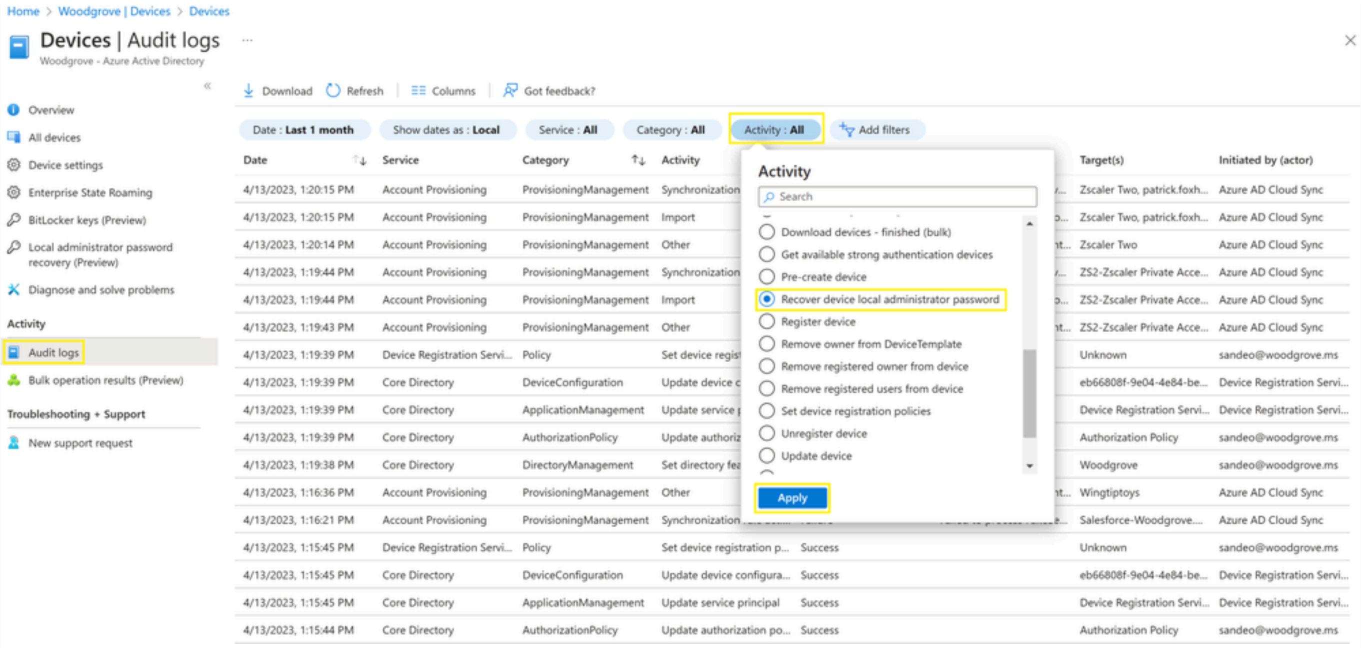

Home > Woodgrove | Devices > Devices
Devices | Audit logs
Woodgrove - Azure Active Directory
Overview
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Download
Refresh
Columns
Got feedback?
Date : Last 1 month
Show dates as : Local
Service : All
Category : All
Activity : All
Add filters
Activity
Search
○ Recover device local administrator password
○ Register device
○ Remove owner from DeviceTemplate
○ Remove registered owner from device
○ Remove registered users from device
○ Set device registration policies
○ Unregister device
○ Update device
○ Update device configuration
○ Update device local administrator
● Update device local administrator password
Apply

Date	Service	Category	Activity	Target(s)	Initiated by (actor)
4/13/2023, 1:19:39 PM	Core Directory	DeviceConfiguration	Update device c	eb66808f-9e04-4e84-be...	Device Registration Servi...
4/13/2023, 1:15:45 PM	Device Registration Servi...	Policy	Set device regist	Unknown	sandeo@woodgrove.ms
4/13/2023, 1:15:45 PM	Core Directory	DeviceConfiguration	Update device c	eb66808f-9e04-4e84-be...	Device Registration Servi...
4/13/2023, 12:58:54 PM	Device Registration Servi...	Device	Recover device l	Win11LAPSAADJ	sandeo@woodgrove.ms
4/13/2023, 12:58:24 PM	Device Registration Servi...	Device	Update device l	Win11LAPSAADJ	
4/13/2023, 12:58:24 PM	Core Directory	Device	Update device	Win11LAPSAADJ	Device Registration Servi...
4/13/2023, 12:52:52 PM	Device Registration Servi...	Policy	Set device regist	Unknown	sandeo@woodgrove.ms
4/13/2023, 12:52:52 PM	Core Directory	DeviceConfiguration	Update device c	eb66808f-9e04-4e84-be...	Device Registration Servi...
4/13/2023, 12:51:48 PM	Device Registration Servi...	Device	Recover device l	Win11LAPSAADJ	sandeo@woodgrove.ms
4/13/2023, 12:39:54 PM	Device Registration Servi...	Device	Recover device l	Win11LAPSAADJ	sandeo@woodgrove.ms
4/13/2023, 11:08:27 AM	Device Registration Servi...	Policy	Set device regist	Unknown	sandeo@woodgrove.ms
4/13/2023, 11:08:27 AM	Core Directory	DeviceConfiguration	Update device c	eb66808f-9e04-4e84-be...	Device Registration Servi...
4/13/2023, 8:24:50 AM	Core Directory	Device	Update device	DESKTOP-SV2H7LN	Device Registration Servi...


Home > Woodgrove | Devices > Devices
Devices | Audit logs
Woodgrove - Azure Active Directory
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
Download
Refresh
Columns
Got feedback?
Add filters

Date : Last 1 month | Show dates as : Local | Service : All | Category : All | Activity : Update device local administrator password

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
4/13/2023, 12:58:24 PM	Device Registration Service	Device	Update device local admi...	Success		Win11LAPSAADJ	
4/4/2023, 10:37:33 PM	Device Registration Service	Device	Update device local admi...	Success		Win11LAPSAADJ	
4/4/2023, 10:34:04 PM	Device Registration Service	Device	Update device local admi...	Success		Win11LAPSAADJ	
3/28/2023, 3:29:19 PM	Device Registration Service	Device	Update device local admi...	Success		Win11LAPSAADJ	
3/27/2023, 9:32:53 AM	Device Registration Service	Device	Update device local admi...	Success		Win11LAPSAADJ	
3/27/2023, 8:45:56 AM	Device Registration Service	Device	Update device local admi...	Success		Win11LAPSAADJ	

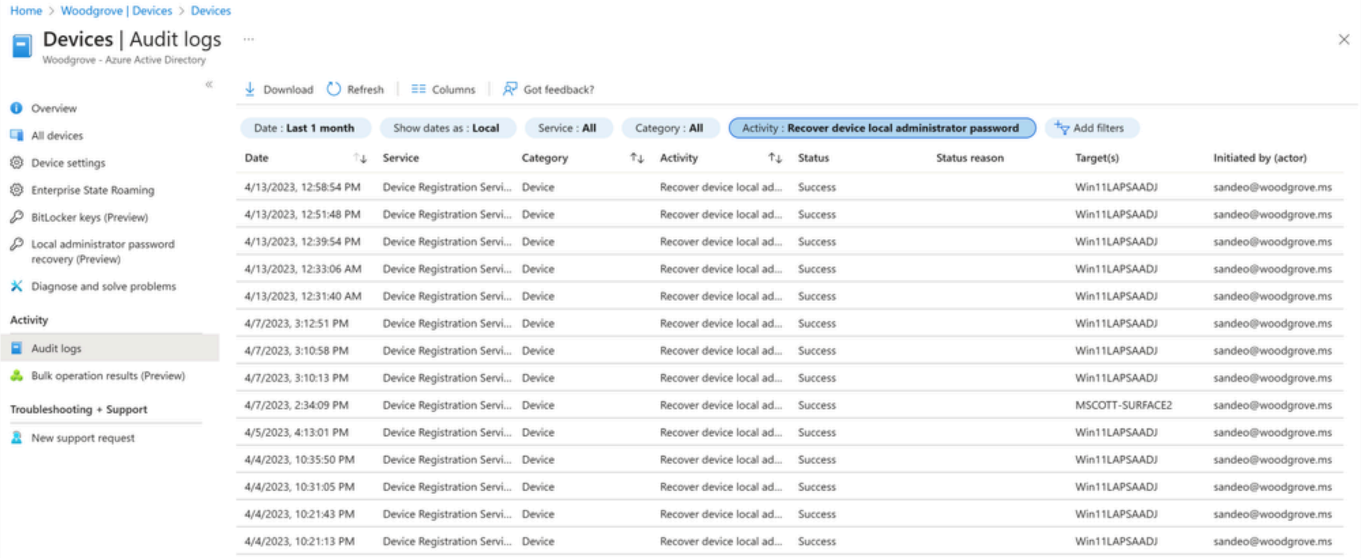

Home > Woodgrove | Devices > Devices
Devices | Audit logs
Woodgrove - Azure Active Directory
Overview
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Download
Refresh
Columns
Got feedback?
Add filters
Apply

Date : **Last 1 month** | Show dates as : **Local** | Service : **All** | Category : **All** | Activity : **All**

Activity

- ○ Download devices - finished (bulk)
- ○ Get available strong authentication devices
- ○ Pre-create device
- ● Recover device local administrator password
- ○ Register device
- ○ Remove owner from DeviceTemplate
- ○ Remove registered owner from device
- ○ Remove registered users from device
- ○ Set device registration policies
- ○ Unregister device
- ○ Update device

Date	Service	Category	Activity		Target(s)	Initiated by (actor)
4/13/2023, 1:20:15 PM	Account Provisioning	ProvisioningManagement	Synchronization		Zscaler Two, patrick.foxh...	Azure AD Cloud Sync
4/13/2023, 1:20:15 PM	Account Provisioning	ProvisioningManagement	Import		Zscaler Two, patrick.foxh...	Azure AD Cloud Sync
4/13/2023, 1:20:14 PM	Account Provisioning	ProvisioningManagement	Other		Zscaler Two	Azure AD Cloud Sync
4/13/2023, 1:19:44 PM	Account Provisioning	ProvisioningManagement	Synchronization		ZS2-Zscaler Private Acce...	Azure AD Cloud Sync
4/13/2023, 1:19:44 PM	Account Provisioning	ProvisioningManagement	Import		ZS2-Zscaler Private Acce...	Azure AD Cloud Sync
4/13/2023, 1:19:43 PM	Account Provisioning	ProvisioningManagement	Other		ZS2-Zscaler Private Acce...	Azure AD Cloud Sync
4/13/2023, 1:19:39 PM	Device Registration Servi...	Policy	Set device regist		Unknown	sandeo@woodgrove.ms
4/13/2023, 1:19:39 PM	Core Directory	DeviceConfiguration	Update device c		eb66808f-9e04-4e84-be...	Device Registration Servi...
4/13/2023, 1:19:39 PM	Core Directory	ApplicationManagement	Update service p		Device Registration Servi...	Device Registration Servi...
4/13/2023, 1:19:39 PM	Core Directory	AuthorizationPolicy	Update authoriz		Authorization Policy	sandeo@woodgrove.ms
4/13/2023, 1:19:38 PM	Core Directory	DirectoryManagement	Set directory fea		Woodgrove	sandeo@woodgrove.ms
4/13/2023, 1:16:36 PM	Account Provisioning	ProvisioningManagement	Other		Wingtiptoys	Azure AD Cloud Sync
4/13/2023, 1:16:21 PM	Account Provisioning	ProvisioningManagement	Synchronization		Salesforce-Woodgrove....	Azure AD Cloud Sync
4/13/2023, 1:15:45 PM	Device Registration Servi...	Policy	Set device registration p...	Success	Unknown	sandeo@woodgrove.ms
4/13/2023, 1:15:45 PM	Core Directory	DeviceConfiguration	Update device configura...	Success	eb66808f-9e04-4e84-be...	Device Registration Servi...
4/13/2023, 1:15:45 PM	Core Directory	ApplicationManagement	Update service principal	Success	Device Registration Servi...	Device Registration Servi...
4/13/2023, 1:15:44 PM	Core Directory	AuthorizationPolicy	Update authorization po...	Success	Authorization Policy	sandeo@woodgrove.ms


Home > Woodgrove | Devices > Devices
Devices | Audit logs
Woodgrove - Azure Active Directory
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
Download
Refresh
Columns
Got feedback?
Add filters

Date : **Last 1 month** | Show dates as : **Local** | Service : **All** | Category : **All** | Activity : **Recover device local administrator password**

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

Skip to Primary Navigation

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

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

Comment

Co-Authors

Alex Simons (AZURE)

Version history

Skip to Primary Navigation

Last update: Apr 24 2023 08:52 AM

Updated by: SHDriggers

Labels

Product Announcements	257

Share

in f 🐦 ✉

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

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Virtual workshops and training

Microsoft Store Promise

Flexible Payments

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

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Skip to Primary Navigation

Microsoft Teams

Microsoft Industry

Small Business

Azure Marketplace

AppSource

Visual Studio

Diversity and inclusion

Accessibility

Sustainability

✓✕ Your Privacy Choices

Sitemap Contact Microsoft Privacy Manage cookies Terms of use Trademarks Safety & eco About our ads