What is Windows LAPS?

Article • 04/12/2023

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. You also can use Windows LAPS to automatically manage and back up the Directory Services Restore Mode (DSRM) account password on your Windows Server Active Directory domain controllers. An authorized administrator can retrieve the DSRM password and use it.

Windows LAPS supported platforms and Azure AD LAPS preview status

Windows LAPS is now available on the following OS platforms with the specified update or later installed:

- Windows 11 22H2 - April 11 2023 Update
- Windows 11 21H2 - April 11 2023 Update
- Windows 10 - April 11 2023 Update
- Windows Server 2022 - April 11 2023 Update
- Windows Server 2019 - April 11 2023 Update

The Windows LAPS on-premises Active Directory scenarios are fully supported as of the above updates.

> ⓘ **Important**
>
> There is a legacy LAPS interop bug in the above April 11, 2023 update. If you install the legacy LAPS GPO CSE on a machine patched with the April 11, 2023 security update and an applied legacy LAPS policy, both Windows LAPS and legacy LAPS will break. Symptoms include Windows LAPS event log IDs 10031 and 10032, as well as legacy LAPS event ID 6. Microsoft is working on a fix for this issue.
>
> You can work around this issue by either: a) uninstalling legacy LAPS, or b) deleting all registry values under the HKLM\Software\Microsoft\Windows\CurrentVersion\LAPS\State registry key.

> ⓘ **Important**

The Azure Active Directory LAPS scenario remains in private preview and is closed to new customers. The Azure Active Directory LAPS scenario is scheduled to enter public preview in Q2 2023. This documentation will be updated once a more precise date for the public preview is available.

Benefits of using Windows LAPS

Use Windows LAPS to regularly rotate and manage local administrator account passwords and get these benefits:

- Protection against pass-the-hash and lateral-traversal attacks
- Improved security for remote help desk scenarios
- Ability to sign in to and recover devices that are otherwise inaccessible
- A fine-grained security model (access control lists and optional password encryption) for securing passwords that are stored in Windows Server Active Directory
- Support for the Azure role-based access control model for securing passwords that are stored in Azure Active Directory

Watch this video to learn about Windows LAPS.
https://www.youtube-nocookie.com/embed/jdEDIXm4JgU

Key Windows LAPS scenarios

You can use Windows LAPS for several primary scenarios:

- Back up local administrator account passwords to Azure Active Directory (for Azure Active Directory-joined devices)

- Back up local administrator account passwords to Windows Server Active Directory (for Windows Server Active Directory-joined clients and servers)

- Back up DSRM account passwords to Windows Server Active Directory (for Windows Server Active Directory domain controllers)

- Back up local administrator account passwords to Windows Server Active Directory by using legacy Microsoft LAPS

In each scenario, you can apply different policy settings.

Understand device join state restrictions

Whether a device is joined to Azure Active Directory or Windows Server Active Directory determines how you can use Windows LAPS.

Devices that are joined only to Azure Active Directory can back up passwords only to Azure Active Directory.

Devices that are joined only to Windows Server Active Directory can back up passwords only to Windows Server Active Directory.

Devices that are hybrid-joined (joined to both Azure Active Directory and Windows Server Active Directory) can back up their passwords either to Azure Active Directory or to Windows Server Active Directory. You can't back up passwords to both Azure Active Directory and Windows Server Active Directory.

Windows LAPS doesn't support Azure Active Directory workplace-joined clients.

Set Windows LAPS policy

To set up and manage policy for your Windows LAPS deployment, you have multiple options:

- Windows LAPS configuration service provider (CSP)
- Windows LAPS Group Policy
- Legacy Microsoft LAPS

Manage and monitor Windows LAPS

You also have various options to manage and monitor Windows LAPS.

Options for Windows include:

- The Windows Server Active Directory Users and Computers properties dialog
- A dedicated event log channel
- A Windows PowerShell module that's specific to Windows LAPS

Azure-based monitoring and reporting solutions are available when you back up passwords to Azure Active Directory.

Windows LAPS vs. legacy Microsoft LAPS

You can still download an earlier version of Local Administrator Password Solution, legacy Microsoft LAPS .

Windows LAPS inherits many design concepts from legacy Microsoft LAPS. If you're familiar with legacy Microsoft LAPS, many Windows LAPS features will be familiar. A key difference is that Windows LAPS is an entirely separate implementation that's native to Windows. Windows LAPS also adds many features that aren't available in legacy Microsoft LAPS. You can use Windows LAPS to back up passwords to Azure Active Directory, encrypt passwords in Windows Server Active Directory, and store your password history.

> ⓘ **Important**
>
> Windows LAPS doesn't require you to install legacy Microsoft LAPS. You can fully deploy and use all Windows LAPS features without installing or referring to legacy Microsoft LAPS. But to help migrate an existing legacy Microsoft LAPS deployment, Windows LAPS offers **legacy Microsoft LAPS emulation mode**.

See also

Legacy Microsoft LAPS

Next steps

- Key concepts in Windows LAPS
- Get started with Windows LAPS for Windows Server Active Directory
- Get started with Windows LAPS for Azure Active Directory
- Get started with Windows LAPS in legacy Microsoft LAPS emulation mode

Key concepts in Windows LAPS

Article • 03/22/2023 • 11 minutes to read

Learn about the basic design and security concepts for Windows Local Administrator Password Solution (Windows LAPS), including:

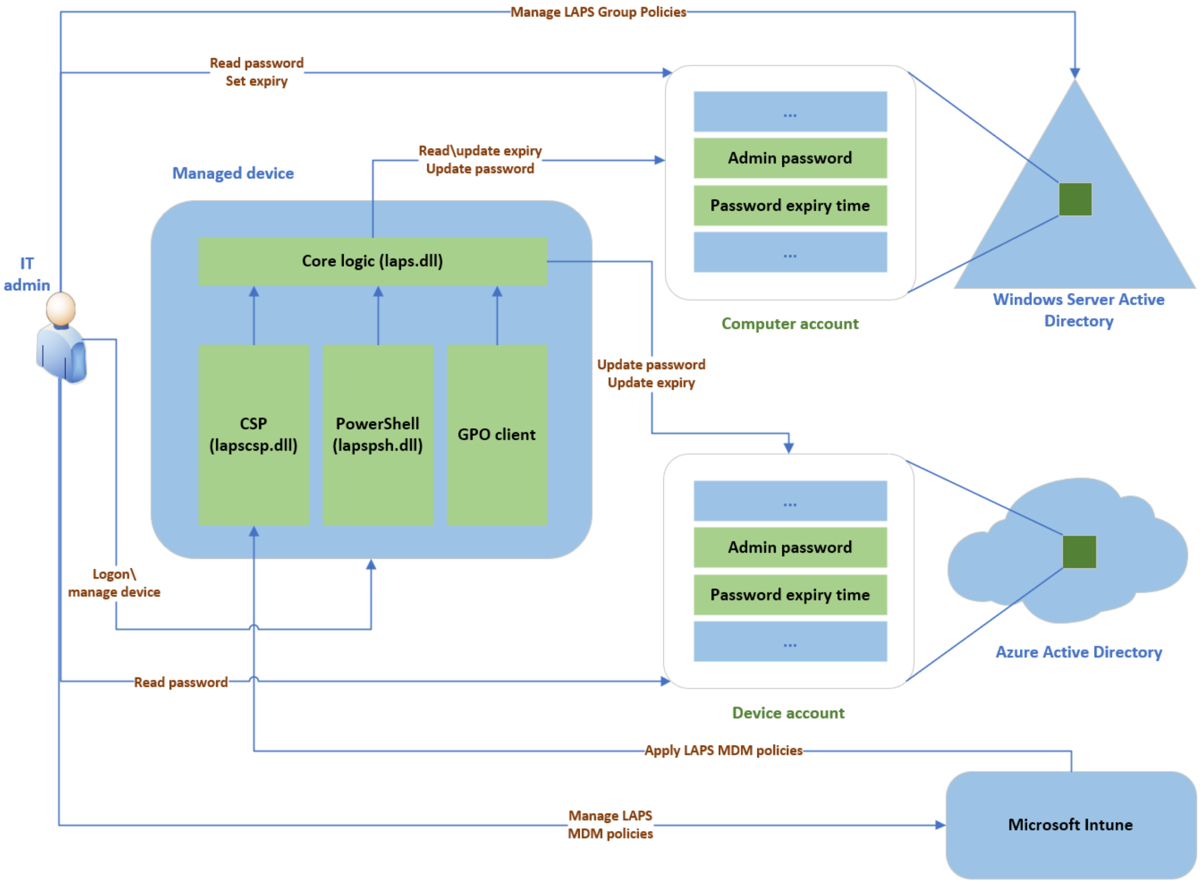
- Architecture
- Basic scenario flow
- Background policy processing cycle
- Azure Active Directory passwords
- Windows Server Active Directory passwords
- Password reset after authentication
- Account password tampering protection
- Windows safe mode

ⓘ **Important**

Windows LAPS currently is available only in **Windows 11 Insider Preview Build 25145 and later** and the Azure Active Directory LAPS scenario is in private preview. For more information see **Windows LAPS availability and Azure AD LAPS public preview status**.

Windows LAPS architecture

The following figure depicts the Windows LAPS architecture:



The Windows LAPS architecture diagram has several key components:

- **IT admin**: Represents collectively the various IT admin roles that might be involved in a Windows LAPS deployment. The IT admin roles are involved with policy configuration, expiration or retrieval of stored passwords, and interacting with managed devices.

- **Managed device**: Represents an Azure Active Directory-joined or Windows Server Active Directory-joined device on which you want to manage a local administrator account. The feature is composed of a few key binaries: *laps.dll* for core logic, *lapscsp.dll* for configuration service provider (CSP) logic, and *lapspsh.dll* for PowerShell cmdlet logic. You also can configure Windows LAPS by using Group Policy. Windows LAPS responds to Group Policy Object (GPO) change notifications. The managed device can be a Windows Server Active Directory domain controller and be configured to back up Directory Services Repair Mode (DSRM) account passwords.

- **Windows Server Active Directory**: An on-premises Windows Server Active Directory deployment.

- **Azure Active Directory**: An Azure Active Directory deployment running in the cloud.

- **Microsoft Intune** The preferred Microsoft device policy management solution, also running in the cloud.

Basic scenario flow

The first step in a basic Windows LAPS scenario is to configure the Windows LAPS policy for your organization. We recommend that you use the following configuration options:

- **Azure Active Directory-joined devices**: Use Microsoft Intune.
- **Windows Server Active Directory-joined devices**: Use Group Policy.
- **Hybrid Azure Active Directory-joined devices that are enrolled with Microsoft Intune**: Use Microsoft Intune.

After the managed device is configured with a policy that enables Windows LAPS, the device begins to manage the configured local account password. When the password expires, the device generates a new, random password that's compliant with the current policy's length and complexity requirements. The password is validated against the local device's password complexity policy.

When a new password is validated, the device stores the password in the configured directory, either Windows Server Active Directory or Azure Active Directory. An associated password expiration time that's based on the current policy's password age setting also is computed and stored in the directory. The device rotates the password automatically when the password expiration time is reached.

When the local account password is stored in the relevant directory, an authorized IT admin can access the password. Passwords that are stored in Azure Active Directory are secured via a role-based access control model. Passwords that are stored in Windows Server Active Directory are secured via access control lists (ACLs) and also optionally via password encryption.

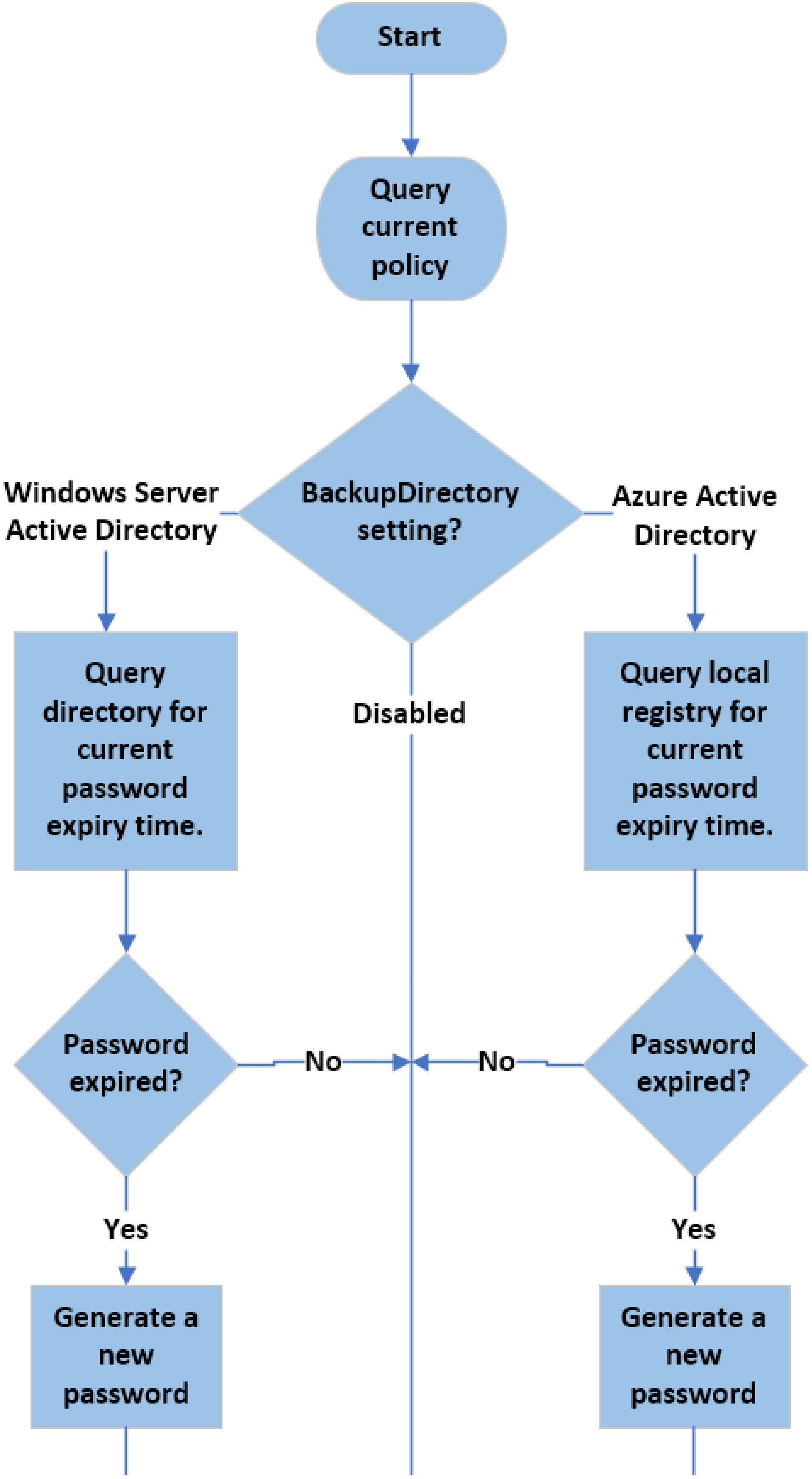
You can rotate the password before the normally expected expiration time. Rotate a password before a scheduled expiration by using one of the following methods:

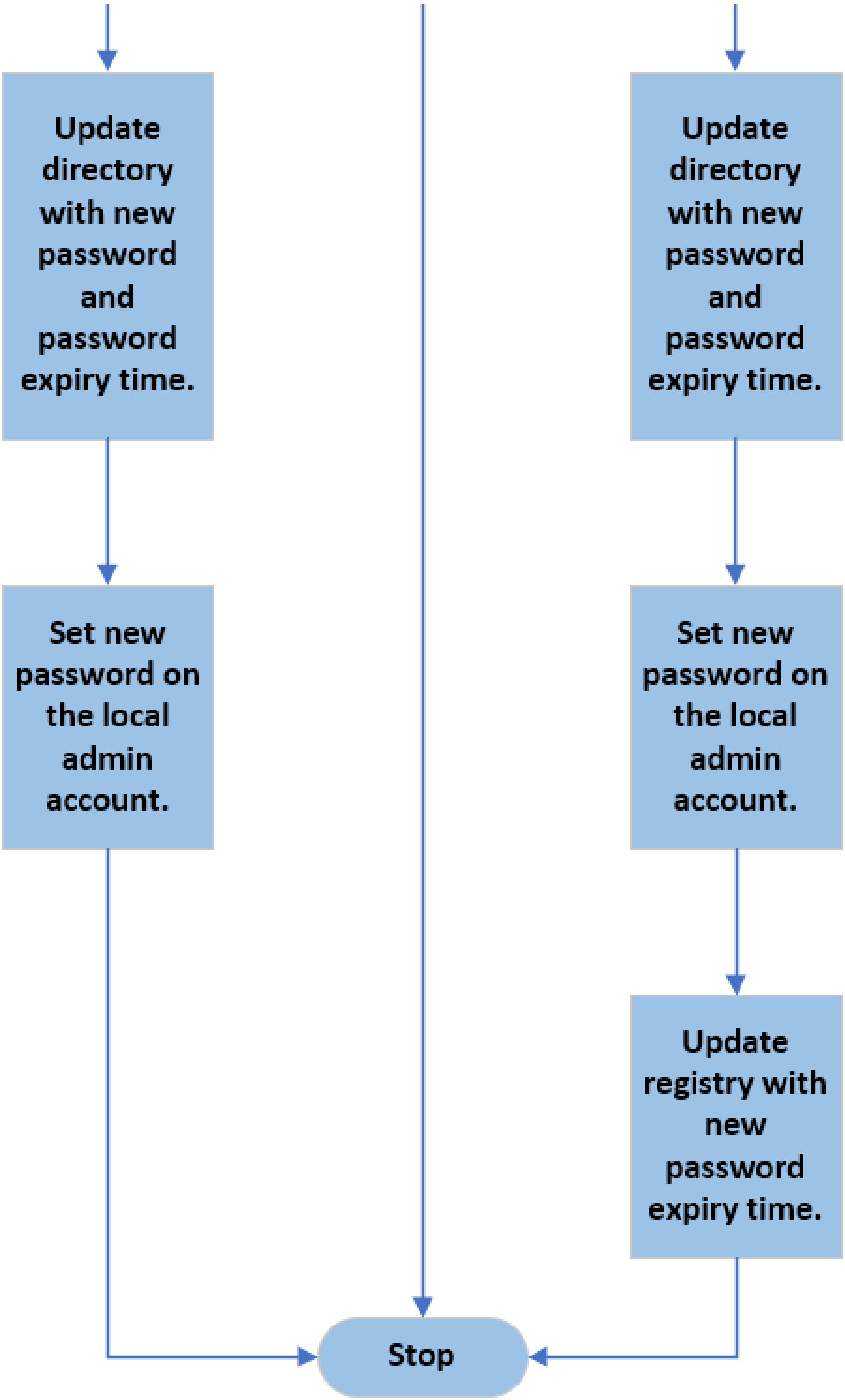
- Manually intervene on the managed device itself by using an admin account. For example, you can use the `Reset-LapsPassword` cmdlet.
- Invoke the ResetPassword Execute action in the Windows LAPS CSP.
- Modify the password expiration time in the directory (applies only to Windows Server Active Directory).
- Trigger automatic rotation when the managed account is used to authenticate to the managed device.

Background policy processing cycle

Windows LAPS uses a background task that wakes up every hour to process the currently active policy. This task isn't implemented by using Windows Task Scheduler.

When the background task runs, it executes the following basic flow:





Update directory with new password and password expiry time.
Update directory with new password and password expiry time.
Set new password on the local admin account.
Set new password on the local admin account.
Update registry with new password expiry time.
Stop

The obvious key difference between the Azure Active Directory flow and the Windows Server Active Directory flow is related to how password expiration time is checked. In both scenarios, password expiration time is stored side-by-side with the latest password in the directory.

In the Azure Active Directory scenario, the managed device doesn't poll Azure Active Directory. Instead, the current password expiration time is maintained locally on the device.

In the Windows Server Active Directory scenario, the managed device regularly polls the directory to query the password expiration time, and it acts when the password expires.

Manually start the policy processing cycle

Windows LAPS does respond to Group Policy change notifications. You can manually start the policy processing cycle in two ways:

- Force a Group Policy refresh. Here's an example:

  PowerShell

  ```
  gpupdate.exe /target:computer /force
  ```

- Run the `Invoke-LapsPolicyProcessing` cmdlet. This method is preferred because it's more scoped.

> **Tip**
>
> The earlier released Microsoft LAPS (legacy Microsoft LAPS) was built as a Group Policy (GPO) Client Side Extension (CSE). GPO CSEs are loaded and invoked in every Group Policy refresh cycle. The frequency of the legacy Microsoft LAPS polling cycle is the same as the frequency of the Group Policy refresh cycle. Windows LAPS is not built as a CSE, so its polling cycle is hard-coded to once per hour. Windows LAPS is not affected by the Group Policy refresh cycle.

Azure Active Directory passwords

When you back up passwords to Azure Active Directory, managed local account passwords are stored on the Azure Active Directory device object. Windows LAPS authenticates to Azure Active Directory by using the device identity of the managed device. Data that's stored in Azure Active Directory is highly secure, but for extra protection, the password is further encrypted before it's persisted. This extra encryption layer is removed before the password is returned to authorized clients.

By default, only members of the Global Administrator, Cloud Device Administrator, and Intune Administrator roles can retrieve the clear-text password.

Windows Server Active Directory passwords

The following sections give you important information about using Windows LAPS with Windows Server Active Directory.

Password security

When you back up passwords to Windows Server Active Directory, managed local account passwords are stored on the computer object. Windows LAPS secures these passwords by using two mechanisms:

- ACLs
- Encrypted passwords

ACLs

The first line of password security in Windows Server Active Directory is ACLs that are set up on the computer object that contains an Organizational Unit (OU). The ACLs are inherited to the computer object itself. You can specify who can read various password attributes by using the `Set-LapsADReadPasswordPermission` cmdlet. Similarly, you can specify who can read and set the password expiration time attribute by using the `Set-LapsADResetPasswordPermission` cmdlet.

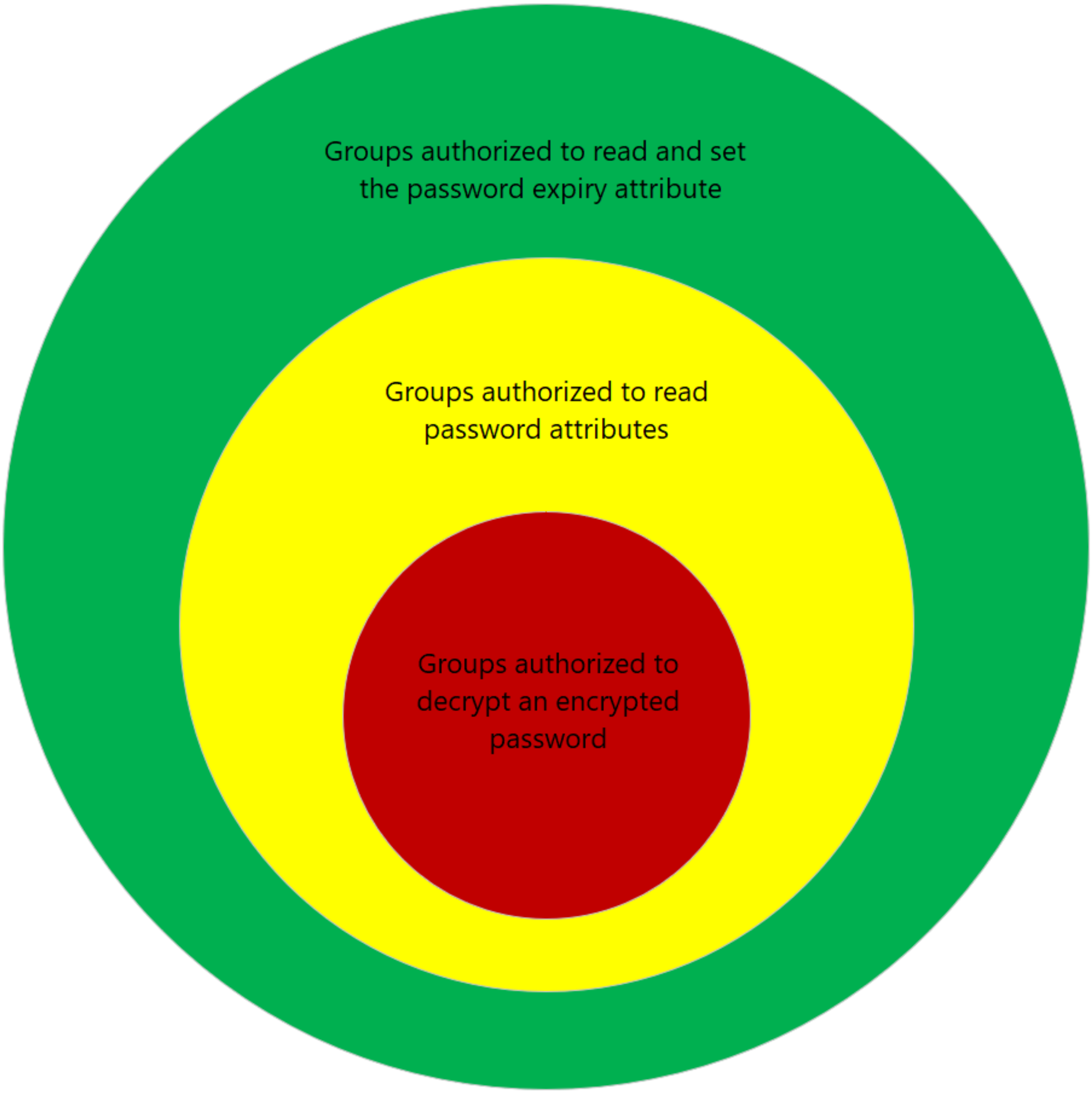
Encrypted passwords

The second line of password security uses the Windows Server Active Directory password encryption feature. To use Windows Server Active Directory password encryption, your domain must run at the Windows Server 2016 Domain Functional Level (DFL) or later. When enabled, the password is first encrypted so that only a specific security principal (a group or user) can decrypt it. The password encryption occurs on the managed device itself before the device sends the password to the directory.

> ⓘ **Important**
>
> - We highly recommend that you enable password encryption when you store your Windows LAPS passwords in Windows Server Active Directory.
> - Microsoft doesn't support retrieval of previously decrypted LAPS passwords in a domain running a DFL earlier than the Windows Server 2016 DFL. The operation might or might not succeed depending on whether domain controllers running versions earlier than Windows Server 2016 were promoted into the domain.

User group permissions

When you design your password retrieval security model, consider the information in the following figure:


Groups authorized to read and set the password expiry attribute
Groups authorized to read password attributes
Groups authorized to decrypt an encrypted password

The diagram illustrates the suggested Windows Server Active Directory password security layers and their relationship to each other.

The outermost circle (green) is composed of security principals that have been granted permission to read or set the password expiration time attribute on computer objects in the directory. This ability is a sensitive permission but is considered non-destructive. An attacker who acquires this permission can force managed devices to rotate their managed devices more frequently.

The middle circle (yellow) is composed of security principals that have been granted permission to read or set password attributes on computer objects in the directory. This ability is a sensitive permission and should be carefully monitored. The most secure approach is to reserve this level of permission for members of the Domain Admins security group.

The inner circle (red) applies only when password encryption is enabled. It's composed of groups or users that have been granted decryption permissions for encrypted password attributes on computer objects in the directory. Like the permission in the middle circle, this ability is a sensitive permission and should be carefully monitored. The most secure approach is to reserve this level of permission for members of the Domain Admins group.

> ⓘ **Important**
>
> Consider customizing your security layers to match the sensitivity of the managed machines in your organization. For example, it might be acceptable for front-line IT worker devices to be accessible to help desk administrators, but you likely will want to set tighter boundaries for corporate executive laptops.

Password encryption

The Windows LAPS password encryption feature is based on the Cryptography API: Next Generation Data Protection API (CNG DPAPI). CNG DPAPI supports multiple encryption modes, but Windows LAPS supports encrypting passwords against only a single Windows Server Active Directory security principal (user or group). The underlying encryption is based on Advanced Encryption Standard 256-bit key (AES-256) encryption.

You can use the ADPasswordEncryptionPrincipal policy setting to set a specific security principal for encrypting the password. If ADPasswordEncryptionPrincipal isn't specified, Windows LAPS encrypts the password against the Domain Admins group of the managed device's domain. Before a managed device encrypts a password, the device always verifies that the specified user or group is resolvable.

> **Tip**
>
> - Windows LAPS supports encrypting passwords against only a single security principal. CNG DPAPI does support encryption against multiple security principals, but this mode isn't supported by Windows LAPS because it causes size bloat of the encrypted password buffers. If you need to grant decryption permissions to multiple security principals, to resolve the constraint, you can create a wrapper group that has all the relevant security principals as members.

- The security principal that's authorized to decrypt the password can't be changed after a password is encrypted.

Encrypted password history

Windows LAPS supports a password history feature for Windows Server Active Directory domain-joined clients and domain controllers. Password history is supported only when password encryption is enabled. Password history isn't supported if you store clear-text passwords in Windows Server Active Directory.

When encrypted password history is enabled and it's time to rotate the password, the managed device first reads the current version of the encrypted password from Windows Server Active Directory. The current password is then added to the password history. Earlier versions of the password in the history are deleted as needed to comply with the configured maximum history limitation.

> **Tip**
>
> For the password history feature to work, the managed device must be granted SELF permissions to read the current version of the encrypted password from Windows Server Active Directory. This requirement is handled automatically when you run the `Set-LapsADComputerSelfPermission` cmdlet.

> **Important**
>
> We recommend that you never grant permissions to a managed device to decrypt an encrypted password for any device, including for the device itself.

DSRM password support

Windows LAPS supports backing up the DSRM account password on Windows Server domain controllers. DSRM account passwords can be backed up only to Windows Server Active Directory and if password encryption is enabled. Otherwise, this feature works almost identically to how encrypted password support works for Windows Server Active Directory-joined clients.

Backing up DSRM passwords to Azure Active Directory isn't supported.

> **Important**

When DSRM password backup is enabled, the current DSRM password for any domain controller is retrievable if at least one domain controller in that domain is accessible.

But consider a catastrophic scenario in which all the domain controllers in a domain are down. In this scenario, no DSRM passwords will be available. For this reason, we recommend that you use Windows LAPS DSRM support as only the first component of a larger domain backup and recovery strategy. We strongly recommend that DSRM passwords be regularly extracted from the directory and backed up to a secure store outside Windows Server Active Directory. Windows LAPS doesn't include an external store backup strategy.

Password reset after authentication

Windows LAPS supports automatically rotating the local administrator account password if it detects that the local administrator account was used for authentication. This feature is intended to bound the amount of time that the clear-text password is usable. You can configure a grace period to give a user time to complete their intended actions.

Account password tampering protection

When Windows LAPS is configured to manage a local administrator account password, that account is protected against accidental or careless tampering. This protection extends to the DSRM account when the account is managed by Windows LAPS on a Windows Server Active Directory domain controller.

Disabled in Windows safe mode

When Windows is started in safe mode, DSRM mode, or in any other non-default boot mode, Windows LAPS is disabled and no passwords are backed up.

See also

- Legacy Microsoft LAPS
- CNG DPAPI
- Microsoft Intune

Next steps

Now that you understand the basic concepts of the Windows LAPS design, get started with one of the following scenarios:

- Get started with Windows LAPS for Windows Server Active Directory
- Get started with Windows LAPS for Azure Active Directory
- Get started with Windows LAPS in legacy Microsoft LAPS emulation mode

Get started with Windows LAPS and Azure Active Directory

Article • 04/11/2023

Learn how to get started with Windows Local Administrator Password Solution (Windows LAPS) and Azure Active Directory. The article describes the basic procedures for using Windows LAPS to back up passwords to Azure Active Directory and how to retrieve them.

> ⓘ **Important**
>
> For more information on specific OS updates required to use the Windows LAPS feature, and the current status of the Azure Active Directory LAPS scenario, see **Windows LAPS availability and Azure AD LAPS public preview status**.

Configure device policy

To configure device policy, complete these tasks:

- Choose a policy deployment mechanism
- Understand policies that apply to Azure Active Directory mode
- Configure specific policies

Choose a policy deployment mechanism

The first step is to choose how to apply policy to your devices.

The preferred option for Azure Active Directory-joined devices is to use Microsoft Intune with the Windows LAPS configuration service provider (CSP).

If your devices are Azure Active Directory-joined but you're not using Microsoft Intune, you can still deploy Windows LAPS for Azure Active Directory. In this scenario, you must deploy policy manually (for example, either by using direct registry modification or by using Local Computer Group Policy). For more information, see Configure Windows LAPS policy settings.

> ⓘ Note

If your devices are hybrid-joined to on-premises Windows Server Active Directory, you can deploy policy by using **Windows LAPS Group Policy**.

Policies that apply to Azure Active Directory mode

The Windows LAPS CSP and Windows LAPS Group Policy object both manage the same settings, but only a subset of these settings applies to Windows LAPS in Azure mode.

The following settings are applicable when backing passwords up to Azure Active Directory:

- BackupDirectory
- PasswordAgeDays
- PasswordComplexity
- PasswordLength
- AdministratorAccountName
- PostAuthenticationResetDelay
- PostAuthenticationActions

More plainly: the Windows Server Active Directory-specific policy settings don't make sense, and aren't supported, when backing the password up to Azure Active Directory.

Configure specific policies

At a minimum, you must configure the BackupDirectory setting to the value 1 (backup passwords to Azure Active Directory).

If you don't configure the AdministratorAccountName setting, Windows LAPS defaults to managing the default built-in local administrator account. This built-in account is automatically identified by its well-known relative identifier (RID) and should never be identified by name. The name of the built-in local administrator account varies depending on the default locale of the device.

If you want to configure a custom local administrator account, you should configure the AdministratorAccountName setting with the name of that account.

ⓘ **Important**

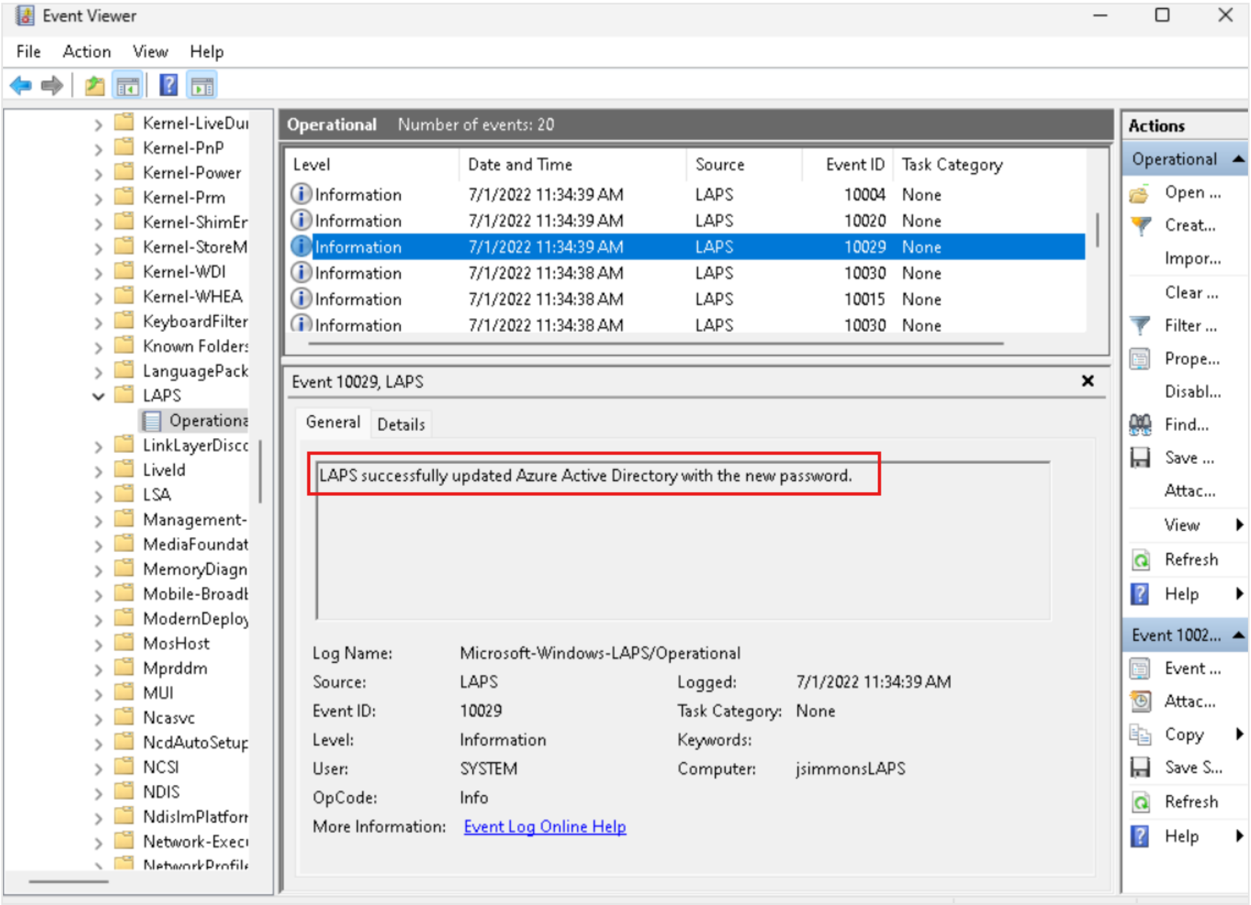
If you configure Windows LAPS to manage a custom local administrator account, you must ensure that the account is created. Windows LAPS doesn't create the account. We recommend that you use the **Accounts CSP** to create the account.

You can configure other settings, like PasswordLength, as needed for your organization.

Update a password in Azure Active Directory

Windows LAPS processes the currently active policy on a periodic basis (every hour). To avoid waiting after you apply the policy, you can run the `Invoke-LapsPolicyProcessing` PowerShell cmdlet.

To verify that the password was successfully updated in Azure Active Directory, look in the event log for the 10029 event:



Operational Number of events: 20

Level	Date and Time	Source	Event ID	Task Category
Information	7/1/2022 11:34:39 AM	LAPS	10004	None
Information	7/1/2022 11:34:39 AM	LAPS	10020	None
Information	7/1/2022 11:34:39 AM	LAPS	10029	None
Information	7/1/2022 11:34:38 AM	LAPS	10030	None
Information	7/1/2022 11:34:38 AM	LAPS	10015	None
Information	7/1/2022 11:34:38 AM	LAPS	10030	None

Event 10029, LAPS

LAPS successfully updated Azure Active Directory with the new password.

Log Name:	Microsoft-Windows-LAPS/Operational		
Source:	LAPS	Logged:	7/1/2022 11:34:39 AM
Event ID:	10029	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	jsimmonsLAPS
OpCode:	Info		
More Information:	Event Log Online Help		

Retrieve a password from Azure Active Directory

Retrieving Windows LAPS passwords stored in Azure Active Directory is supported by using Microsoft Graph. Windows LAPS includes a PowerShell cmdlet (`Get-LapsAADPassword`) that's a wrapper around the Microsoft Graph PowerShell library. Windows LAPS doesn't provide any user interface options for Azure Active Directory password retrieval. The instructions describe how to use the `Get-LapsAADPassword` cmdlet to retrieve Windows LAPS passwords from Azure Active Directory.

Install the Microsoft Graph PowerShell library

The first step is to install the Microsoft Graph PowerShell library:

```
Install-Module Microsoft.Graph -Scope AllUsers
```

You might need to configure the repository as Trusted for the command to succeed:

```
Set-PSRepository PSGallery -InstallationPolicy Trusted
```

Create an Azure Active Directory registered app to retrieve Windows LAPS passwords

The next step is to create an Azure Active Directory application that's configured with the necessary permissions. To review the basic instructions for creating an Azure Active Directory application, see Quickstart: Register an application with the Microsoft identity platform

The app needs to be configured with two permissions: `Device.Read.All` and either `Device.LocalCredentials.Read` or `Device.LocalCredentials.ReadAll`.

> **Important**
>
> - Use `Device.LocalCredentials.Read` to grant permissions for reading non-sensitive metadata about persisted Windows LAPS passwords. Examples include the time the password was backed up to Azure and the expected expiration time of a password. This permissions level is appropriate for reporting and compliance applications.
> - Use `Device.LocalCredentials.ReadAll` to grant full permissions for reading everything about persisted Windows LAPS passwords, including the clear-text passwords themselves. This permissions level is sensitive and should be used carefully.

Manual consent to Device.LocalCredentials.* permissions

Currently, a manual step is required to consent to either `Device.LocalCredentials.Read` or the `Device.LocalCredentials.ReadAll` permissions.

After you decide which `Device.LocalCredentials` permission to configure, manually construct a URL for your scenario. In the following examples, `DeviceLocalCredential.Read.All` is the permission. Replace the permission with `DeviceLocalCredential.Read.Basic` if necessary.

For multi-tenant apps:

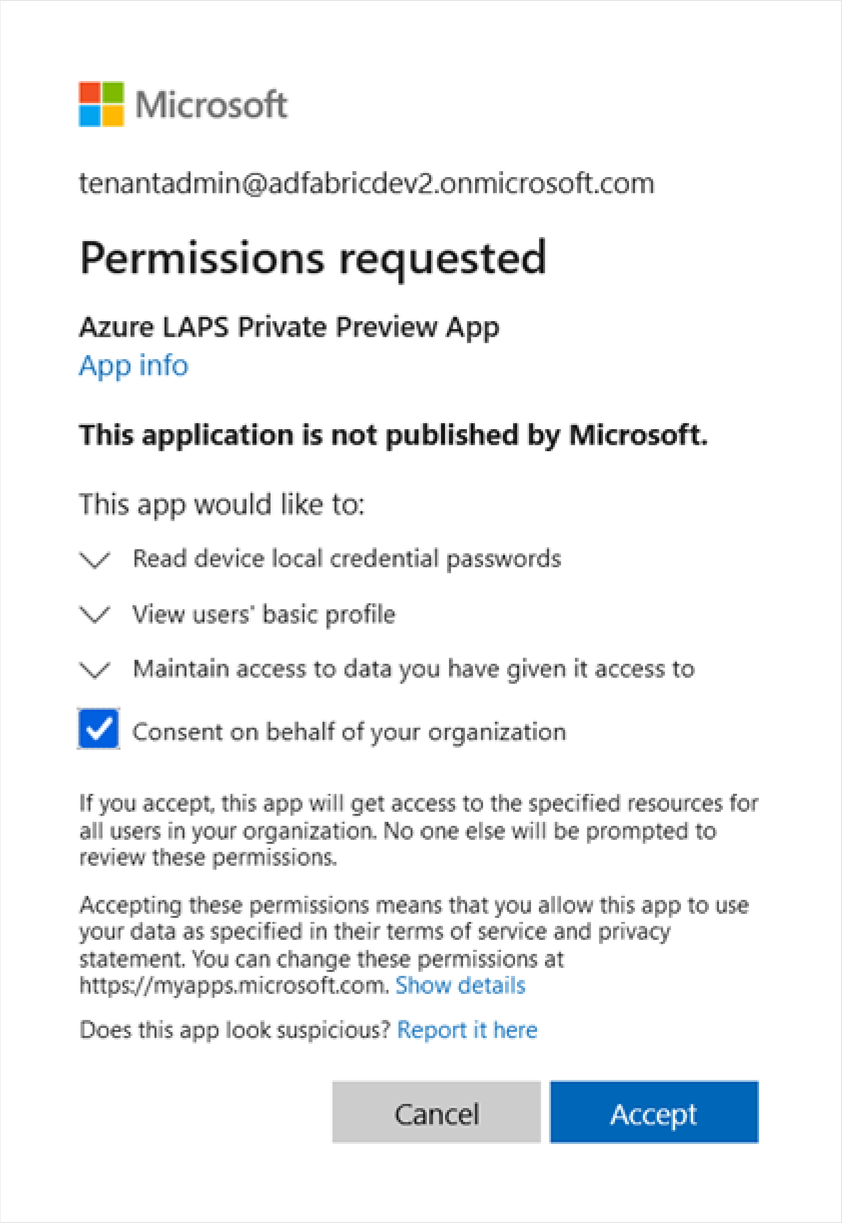
`https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=<YourClientAppID>=response_type=code&scope=https://graph.microsoft.com/DeviceLocalCredential.Read.All`

For single-tenant apps:

`https://login.microsoftonline.com/<YourTenantNameOrTenantID>/oauth2/v2.0/authorize?client_id=<YourClientAppID>&response_type=code&scope=https://graph.microsoft.com/DeviceLocalCredential.Read.All`

Using the URL template that's relevant for your scenario, replace `<YourClientAppID>` with the application ID of the Azure registered app you created earlier. Replace `<YourTenantNameOrTenantID>` with your Azure tenant name or tenant ID.

When the final URL is ready, paste it into a browser and go to the URL. The browser displays a permissions consent dialog. Select the **Consent on behalf of your organization** checkbox, and then select **Accept**. For example:



Microsoft

tenantadmin@adfabricdev2.onmicrosoft.com

Permissions requested

Azure LAPS Private Preview App

App info

This application is not published by Microsoft.

This app would like to:

- Read device local credential passwords
- View users' basic profile
- Maintain access to data you have given it access to

☑ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Retrieve the password from Azure Active Directory

You're almost there! First, sign in to Microsoft Graph. Then, use the `Get-LapsAADPassword` cmdlet to retrieve the password.

To sign in to Microsoft Graph, use the `Connect-MgGraph` cmdlet. You must know your Azure tenant ID and the application ID of the Azure Active Directory application you created earlier. Run the cmdlet once to sign in. For example:

PowerShell

```powershell
PS C:\> Connect-MgGraph -Environment Global -TenantId acca2622-272f-413f-865f-a67416923a6b -ClientId 1c2e514c-2ef1-486d-adbb-8da208457957
```

Output

```
Welcome To Microsoft Graph!
```

Tip

For the `Connect-MgGraph` cmdlet to succeed, you might need to modify your PowerShell execution policy. For example, you might need for first run `Set-ExecutionPolicy -ExecutionPolicy Unrestricted`.

Now that you're logged into Microsoft Graph, you can retrieve the password.

First, invoke the `Get-LapsAADPassword` cmdlet and pass the name of the device:

PowerShell

```
PS C:\> Get-LapsAADPassword -DeviceIds myAzureDevice
```

Output

```
DeviceName    DeviceId                             PasswordExpirationTime
----------    --------                             ----------------------
myAzureDevice be8ab291-6307-42a2-8fda-2f4ee78e51c8 7/31/2022 11:34:39 AM
```

Tip

Pass the `-Verbose` parameter to see detailed info about what the `Get-LapsAADPassword` cmdlet (or any other cmdlet in the Windows LAPS PowerShell module) is doing.

The preceding example requires that the client is granted `DeviceLocalCredential.Read.Basic` permissions. The following examples require that the client is granted `DeviceLocalCredential.Read.All` permissions.

Next, invoke the `Get-LapsAADPassword` cmdlet to ask for the actual password to be returned:

PowerShell

```
PS C:\> Get-LapsAADPassword -DeviceIds myAzureDevice -IncludePasswords
```

Output

```
DeviceName             : myAzureDevice
DeviceId               : be8ab291-6307-42a2-8fda-2f4ee78e51c8
Account                : Administrator
Password               : System.Security.SecureString
PasswordExpirationTime : 7/31/2022 11:34:39 AM
PasswordUpdateTime     : 7/1/2022 11:34:39 AM
```

The password that's returned in a `SecureString` object.

Finally, for testing or ad-hoc purposes, you can request that the password appear in clear text by using the `-AsPlainText` parameter:

PowerShell

```
PS C:\> Get-LapsAADPassword -DeviceIds myAzureDevice -IncludePasswords -
AsPlainText
```

Output

```
DeviceName             : myAzureDevice
DeviceId               : be8ab291-6307-42a2-8fda-2f4ee78e51c8
Account                : Administrator
Password               : xzYVg,;rqQ+rkXEM0B29l3z!Ez.}T9rY8%67i1#TUk
PasswordExpirationTime : 7/31/2022 11:34:39 AM
PasswordUpdateTime     : 7/1/2022 11:34:39 AM
```

Rotate the password

Windows LAPS locally remembers when the last stored password expires, and it automatically rotates the password when the password expires. In some situations (for example, after a security breach or for ad-hoc testing), you might need to rotate the password early. To manually force a password rotation, you can use the `Reset-LapsPassword` cmdlet. For example:

PowerShell

```
PS C:\> Reset-LapsPassword
PS C:\> Get-LapsAADPassword -DeviceIds myAzureDevice -IncludePasswords -
AsPlainText
```

Output

```
DeviceName             : myAzureDevice
DeviceId               : be8ab291-6307-42a2-8fda-2f4ee78e51c8
```

```
Account                : Administrator
Password               : &HK%tbA+k7,vcrI387k9([f+%w)9VZz98;,(@+Ai6b
PasswordExpirationTime : 7/31/2022 12:16:16 PM
PasswordUpdateTime     : 7/1/2022 12:16:16 PM
```

> ⓘ **Important**
>
> - Azure Active Directory doesn't support expiration of a device's currently stored password via modification of the password expiration timestamp in Azure Active Directory. This is a design difference from the Windows Server Active Directory-based Windows LAPS.
> - Avoid excessively frequent use of the `Reset-LapsPassword` cmdlet. If detected, the activity might be throttled.

See also

- Windows LAPS CSP
- Quickstart: Register an application with the Microsoft identity platform

Next steps

- Configure Windows LAPS policy settings
- Use Windows LAPS event logs
- Key concepts in Windows LAPS

Get started with Windows LAPS and Windows Server Active Directory

Article • 04/11/2023

Learn how to get started with Windows Local Administrator Password Solution (Windows LAPS) and Windows Server Active Directory. The article describes the basic procedures for using Windows LAPS to back up passwords to Windows Server Active Directory and how to retrieve them.

> ⓘ **Important**
>
> For more information on specific OS updates required to use the Windows LAPS feature, and the current status of the Azure Active Directory LAPS scenario, see **Windows LAPS availability and Azure AD LAPS public preview status**.

Update the Windows Server Active Directory schema

The Windows Server Active Directory schema must be updated prior to using Windows LAPS. This action is performed by using the `Update-LapsADSchema` cmdlet. It's a one-time operation for the entire forest.

PowerShell

```
PS C:\> Update-LapsADSchema
```

> **Tip**
>
> Pass the `-Verbose` parameter to see detailed info on what the `Update-LapsADSchema` cmdlet (or any other cmdlet in the LAPS PowerShell module) is doing.

Grant the managed device permission to update its password

The managed device needs to be granted permission to update its password. This action is performed by setting inheritable permissions on the Organizational Unit (OU) the device is in. The `Set-LapsADComputerSelfPermission` is used for this purpose, for example:

PowerShell

```
PS C:\> Set-LapsADComputerSelfPermission -Identity NewLaps
```

Output

```
Name    DistinguishedName
----    -----------------
NewLAPS OU=NewLAPS,DC=laps,DC=com
```

Remove Extended Rights permissions

Some users or groups might already be granted Extended Rights permission on the managed device's OU. This permission is problematic because it grants the ability to read confidential attributes (all of the Windows LAPS password attributes are marked as confidential). One way to check to see who is granted these permissions is by using the `Find-LapsADExtendedRights` cmdlet. For example:

PowerShell

```
PS C:\> Find-LapsADExtendedRights -Identity newlaps
```

Output

```
ObjectDN                  ExtendedRightHolders
--------                  --------------------
OU=NewLAPS,DC=laps,DC=com {NT AUTHORITY\SYSTEM, LAPS\Domain Admins}
```

In the output in this example, only trusted entities (SYSTEM and Domain Admins) have the privilege. No other action is required.

Configure device policy

Complete a few steps to configure the device policy.

Choose a policy deployment mechanism

The first step is to choose how to apply policy to your devices.

Most environments use Windows LAPS Group Policy to deploy the required settings to their Windows Server Active Directory-domain-joined devices.

If your devices are also hybrid-joined to Azure Active Directory, you can deploy policy by using Microsoft Intune with the Windows LAPS configuration service provider (CSP).

Configure specific policies

At a minimum, you must configure the BackupDirectory setting to the value 2 (backup passwords to Windows Server Active Directory).

If you don't configure the AdministratorAccountName setting, Windows LAPS defaults to managing the default built-in local administrator account. This built-in account is automatically identified by its well-known relative identifier (RID) and should never be identified by name. The name of the built-in local administrator account varies depending on the default locale of the device.

If you want to configure a custom local administrator account, you should configure the AdministratorAccountName setting with the name of that account.

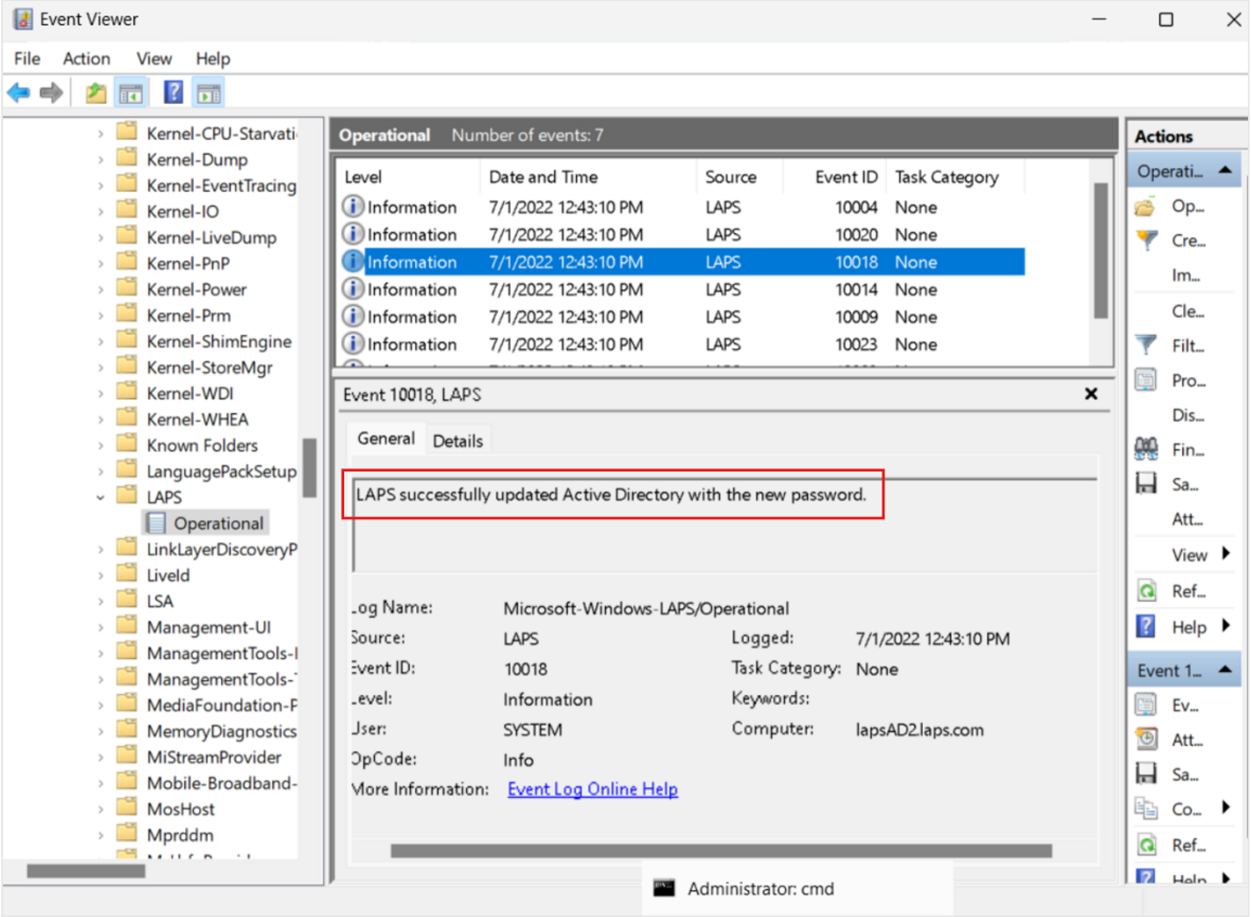
> ⓘ **Important**
>
> If you configure Windows LAPS to manage a custom local administrator account, you must ensure that the account is created. Windows LAPS doesn't create the account. We recommend that you use the **RestrictedGroups CSP** to create the account.

You can configure other settings, like PasswordLength, as needed for your organization.

Update a password in Windows Server Active Directory

Windows LAPS processes the currently active policy on a periodic basis (every hour) and responds to Group Policy change notifications. It responds based on the policy and change notifications.

To verify that the password was successfully updated in Windows Server Active Directory, look in the event log for the 10018 event:



Operational Number of events: 7

Level	Date and Time	Source	Event ID	Task Category
Information	7/1/2022 12:43:10 PM	LAPS	10004	None
Information	7/1/2022 12:43:10 PM	LAPS	10020	None
Information	7/1/2022 12:43:10 PM	LAPS	10018	None
Information	7/1/2022 12:43:10 PM	LAPS	10014	None
Information	7/1/2022 12:43:10 PM	LAPS	10009	None
Information	7/1/2022 12:43:10 PM	LAPS	10023	None

Event 10018, LAPS

General Details

LAPS successfully updated Active Directory with the new password.

Log Name: Microsoft-Windows-LAPS/Operational
Source: LAPS Logged: 7/1/2022 12:43:10 PM
Event ID: 10018 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: lapsAD2.laps.com
OpCode: Info
More Information: Event Log Online Help

To avoid waiting after you apply the policy, you can run the `Invoke-LapsPolicyProcessing` PowerShell cmdlet.

Retrieve a password from Windows Server Active Directory

Use the `Get-LapsADPassword` cmdlet to retrieve passwords from Windows Server Active Directory. For example:

PowerShell

```
PS C:\> Get-LapsADPassword -Identity lapsAD2 -AsPlainText
```

Output

```
ComputerName        : LAPSAD2
DistinguishedName   : CN=LAPSAD2,OU=NewLAPS,DC=laps,DC=com
Account             : Administrator
Password            : Zlh+lzC[0e0/VU
PasswordUpdateTime  : 7/1/2022 1:23:19 PM
ExpirationTimestamp : 7/31/2022 1:23:19 PM
Source              : EncryptedPassword
```

```
DecryptionStatus    : Success
AuthorizedDecryptor : LAPS\Domain Admins
```

This output result indicates that password encryption is enabled (see `Source`). Password encryption requires that your domain is configured for Windows Server 2016 Domain Functional Level or later.

Rotate the password

Windows LAPS reads the password expiration time from Windows Server Active Directory during each policy processing cycle. If the password has expired, a new password is generated and stored immediately.

In some situations (for example, after a security breach or for ad-hoc testing), you might want to rotate the password early. To manually force a password rotation, you can use the `Reset-LapsPassword` cmdlet.

You can use the `Set-LapsADPasswordExpirationTime` cmdlet to set the scheduled password expiration time as stored in Windows Server Active Directory. For example:

PowerShell

```
PS C:\> Set-LapsADPasswordExpirationTime -Identity lapsAD2
```

Output

```
DistinguishedName                            Status
-----------------                            ------
CN=LAPSAD2,OU=NewLAPS,DC=laps,DC=com PasswordReset
```

The next time Windows LAPS wakes up to process the current policy, it sees the modified password expiration time and rotates the password. If you don't want to wait, you can run the `Invoke-LapsPolicyProcessing` cmdlet.

You can use the `Reset-LapsPassword` cmdlet to locally force an immediate rotation of the password.

See also

- RestrictedGroups CSP
- Windows LAPS CSP
- Microsoft Intune

Next steps

- Configure Windows LAPS policy settings
- Use Windows LAPS event logs
- Use Windows LAPS PowerShell cmdlets
- Key concepts in Windows LAPS

Get started with Windows LAPS in legacy Microsoft LAPS emulation mode

Article • 04/11/2023

You can set up Windows Local Administrator Password Solution (Windows LAPS) to honor legacy Microsoft LAPS Group Policy settings, but with some restrictions and limitations. The feature is called *legacy Microsoft LAPS emulation mode*. You might use emulation mode if you migrate an existing deployment of legacy Microsoft LAPS to Windows LAPS.

Like Microsoft LAPS, emulation mode supports storage of passwords in Windows Server Active Directory only in clear-text form. To increase security, we recommend that you migrate to using Windows LAPS natively so that you can take advantage of password encryption.

> ⓘ **Important**
>
> For more information on specific OS updates required to use the Windows LAPS feature, and the current status of the Azure Active Directory LAPS scenario, see **Windows LAPS availability and Azure AD LAPS public preview status**.

Setup and configuration

When you configure Windows LAPS in legacy Microsoft LAPS emulation mode, Windows LAPS assumes that your Windows Server Active Directory environment is set up to run legacy Microsoft LAPS. For more information about legacy Microsoft LAPS configuration, see the legacy Microsoft LAPS documentation.

Requirements and limitations

The following requirements and limitations apply to legacy Microsoft LAPS emulation mode support:

- Windows LAPS doesn't support adding the legacy Microsoft LAPS Windows Server Active Directory schema.

  You must install legacy Microsoft LAPS on a domain controller or another management client to extend your Windows Server Active Directory schema with the legacy Microsoft LAPS schema elements. Use the `Update-AdmPwdADSchema` cmdlet to extend the schema. The Windows LAPS `Update-LapsADSchema` cmdlet doesn't add the legacy Microsoft LAPS schema elements.

- Windows LAPS doesn't install the legacy Microsoft LAPS Group Policy definition files.

  To define and administer legacy Microsoft LAPS group policies, you must install legacy Microsoft LAPS on a domain controller or another management client.

- Windows LAPS doesn't support managing legacy Microsoft LAPS Active Directory access control lists (ACLs).

  To manage the legacy Microsoft LAPS Windows Server Active Directory ACLs, you must install legacy Microsoft LAPS on a domain controller or another management client. For example, to use the `Set-AdmPwdComputerSelfPermissions` cmdlet.

- No other Windows LAPS policies can be applied to the machine.

  If a Windows LAPS policy is present on the machine, it always takes precedence, regardless of how it was applied (configuration service provider, Group Policy Object, or raw registry modification). If a Windows LAPS policy is present, a legacy Microsoft LAPS policy is always ignored. For more information, see Windows LAPS policy settings.

- Legacy Microsoft LAPS must not be installed on the machine.

  This restriction avoids a scenario in which Windows LAPS and legacy Microsoft LAPS simultaneously try to manage the same local administrator account. Having two entities manage the same account is a security risk and isn't supported.

  For the emulation feature, legacy Microsoft LAPS is considered installed if the legacy Microsoft LAPS Group Policy Client Side Extension is installed. To detect the extension, query the `DllName` registry value under this registry key:

  `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}`

  When the DllName value is present and the value refers to a file on disk (the file isn't loaded or otherwise verified), legacy Microsoft LAPS is considered to be installed.

- The Windows Server Active Directory Users and Computer management console doesn't support reading or writing legacy Microsoft LAPS schema attributes.

- Windows LAPS always ignores a legacy Microsoft LAPS policy when Windows LAPS is configured on a Windows Server Active Directory domain controller, even if all other conditions are met.

- All Windows LAPS policy knobs that aren't supported by legacy Microsoft LAPS default to their disabled or default settings.

  For example, when you run Windows LAPS in legacy Microsoft LAPS emulation mode, you can't configure Windows LAPS to do tasks like encrypt passwords or save passwords to Azure Active Directory.

If all these constraints are satisfied, Windows LAPS honors legacy Microsoft LAPS Group Policy settings. The specified managed local administrator account is managed identically to how it's managed in legacy Microsoft LAPS.

Limited administrative support

The `Get-LapsADPassword` cmdlet supports retrieval of the legacy Microsoft LAPS password attribute (`ms-Mcs-AdmPwd`). The `Account` and `PasswordUpdateTime` fields in the resulting output are always blank. For example:

PowerShell

```
PS C:\> Get-LapsADPassword -Identity lapsAD2 -AsPlainText
```

Output

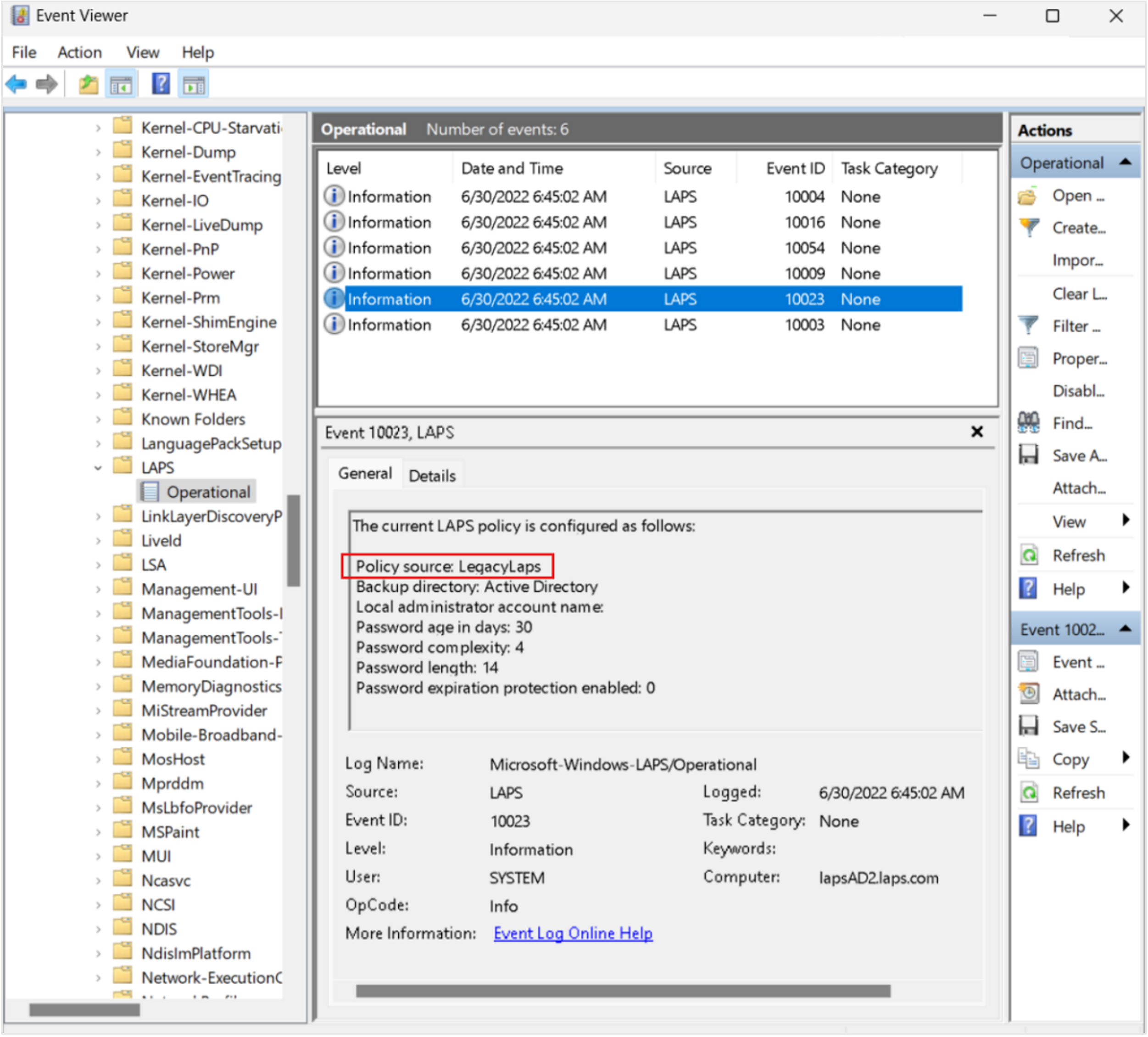
```
ComputerName        : LAPSAD2
DistinguishedName   : CN=LAPSAD2,OU=LapsTestOU,DC=laps,DC=com
Account             :
Password            : SV6[y1n3JG+3l8
PasswordUpdateTime  :
ExpirationTimestamp : 7/31/2022 12:43:10 PM
Source              : CleartextPassword
DecryptionStatus    : NotApplicable
AuthorizedDecryptor : NotApplicable
```

The `Set-LapsADPasswordExpirationTime` cmdlet doesn't support expiring or modifying the legacy Microsoft LAPS password expiration attribute (`ms-Mcs-AdmPwdExpirationTime`).

The Windows LAPS property page in the Windows Server Active Directory Users and Computers management console doesn't support displaying or administering legacy Microsoft LAPS attributes.

Logging

When Windows LAPS runs in legacy Microsoft LAPS emulation mode, a 10023 event is logged to detail the current policy configuration:



Operational Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	6/30/2022 6:45:02 AM	LAPS	10004	None
Information	6/30/2022 6:45:02 AM	LAPS	10016	None
Information	6/30/2022 6:45:02 AM	LAPS	10054	None
Information	6/30/2022 6:45:02 AM	LAPS	10009	None
Information	6/30/2022 6:45:02 AM	LAPS	10023	None
Information	6/30/2022 6:45:02 AM	LAPS	10003	None

Event 10023, LAPS

```
The current LAPS policy is configured as follows:

Policy source: LegacyLaps
Backup directory: Active Directory
Local administrator account name:
Password age in days: 30
Password complexity: 4
Password length: 14
Password expiration protection enabled: 0
```

```
Log Name:          Microsoft-Windows-LAPS/Operational
Source:            LAPS                  Logged:          6/30/2022 6:45:02 AM
Event ID:          10023                 Task Category:   None
Level:             Information           Keywords:
User:              SYSTEM                Computer:        lapsAD2.laps.com
OpCode:            Info
More Information:  Event Log Online Help
```

Otherwise, the same events that are logged by Windows LAPS when it doesn't run in legacy Microsoft LAPS emulation mode are also logged when it runs in legacy Microsoft LAPS emulation mode.

See also

This article doesn't go into detail about managing other aspects of legacy Microsoft LAPS. For more information, see the legacy Microsoft LAPS documentation on the download page:

- Legacy Microsoft LAPS

Next steps

- Configure Windows LAPS policy settings

Configure policy settings for Windows LAPS

Article • 03/24/2023 • 7 minutes to read

Windows Local Administrator Password Solution (Windows LAPS) supports various settings you can control by using policy. Learn about the settings and how to administer them.

> ⓘ **Important**
>
> Windows LAPS currently is available only in **Windows 11 Insider Preview Build 25145 and later** and the Azure Active Directory LAPS scenario is in private preview. For more information see **Windows LAPS availability and Azure AD LAPS public preview status**.

Supported policy roots

Although we don't recommend it, you can administer a device by using multiple policy management mechanisms. To support this scenario in an understandable and predictable way, each Windows LAPS policy mechanism is assigned a distinct registry root key:

Policy name	Policy registry key root
LAPS CSP	`HKLM\Software\Microsoft\Policies\LAPS`
LAPS Group Policy	`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS`
LAPS Local Configuration	`HKLM\Software\Microsoft\Windows\CurrentVersion\LAPS\Config`
Legacy Microsoft LAPS	`HKLM\Software\Policies\Microsoft Services\AdmPwd`

Windows LAPS queries all known registry key policy roots, starting at the top and moving down. If no settings are found under a root, that root is skipped and the query proceeds to the next root. When a root that has at least one explicitly defined setting is found, that root is used as the active policy. If the chosen root is missing any settings, the settings are assigned their default values.

Policy settings are never shared or inherited across policy key roots.

💡 Tip

The LAPS Local Configuration key is included in the preceding table for completeness. You can use this key if necessary, but the key primarily is intended to be used for testing and development. No management tools or policy mechanisms target this key.

Supported policy settings by join state

Windows LAPS supports multiple policy settings that you can administer via various policy management solutions, or even directly via the registry.

The following table specifies which settings apply to devices that have the specified join state:

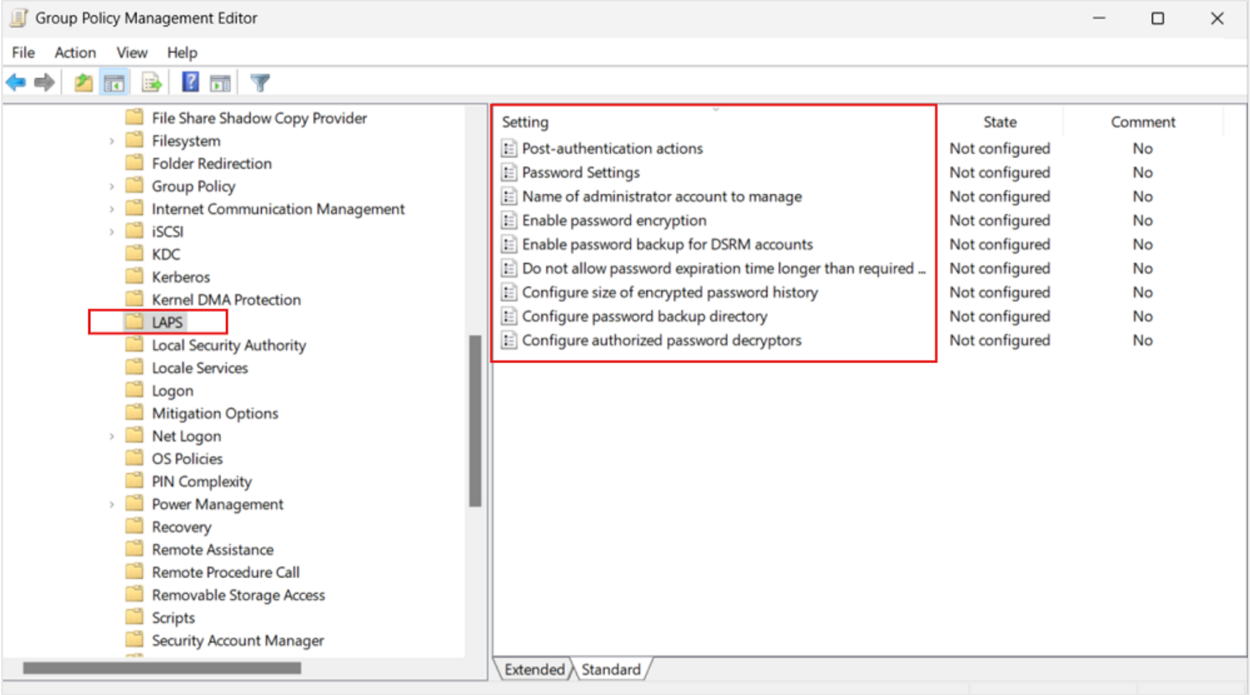
Setting name	Azure Active Directory-joined	Hybrid-joined	Windows Server Active Directory-joined
BackupDirectory	Yes	Yes	Yes
PasswordAgeDays	Yes	Yes	Yes
PasswordLength	Yes	Yes	Yes
PasswordComplexity	Yes	Yes	Yes
PasswordExpirationProtectionEnabled	No	Yes	Yes
AdministratorAccountName	Yes	Yes	Yes
ADPasswordEncryptionEnabled	No	Yes	Yes
ADPasswordEncryptionPrincipal	No	Yes	Yes
ADEncryptedPasswordHistorySize	No	Yes	Yes
ADBackupDSRMPassword	No	No	Yes
PostAuthenticationResetDelay	Yes	Yes	Yes
PostAuthenticationActions	Yes	Yes	Yes

You can administer almost all settings by using any policy management mechanism. The Windows LAPS configuration service provider (CSP) has two exceptions to this rule. The Windows LAPS CSP supports two settings that aren't in the preceding table: ResetPassword and ResetPasswordStatus. Also, Windows LAPS CSP doesn't support the

ADBackupDSRMPassword setting (domain controllers are never managed via CSP). For more information, see the LAPS CSP documentation.

Windows LAPS Group Policy

Windows LAPS includes a new Group Policy Object that you can use to administer policy settings on Active Directory domain-joined devices. To access the Windows LAPS Group Policy, in Group Policy Management Editor, go to **Computer Configuration** > **Administrative Templates** > **System** > **LAPS**. The following figure shows an example:



Setting	State	Comment
Post-authentication actions	Not configured	No
Password Settings	Not configured	No
Name of administrator account to manage	Not configured	No
Enable password encryption	Not configured	No
Enable password backup for DSRM accounts	Not configured	No
Do not allow password expiration time longer than required ...	Not configured	No
Configure size of encrypted password history	Not configured	No
Configure password backup directory	Not configured	No
Configure authorized password decryptors	Not configured	No

Windows LAPS CSP

Windows LAPS includes a specific CSP that you can use to administer policy settings on Azure Active Directory-joined devices. Manage the Windows LAPS CSP by using Microsoft Intune.

Apply policy settings

The following sections describe how to use and apply various policy settings for Windows LAPS.

BackupDirectory

Use this setting to control which directory the password for the managed account is backed up to.

Value	Description of setting
0	Disabled (password won't be backed up)
1	Back up the password to Azure Active Directory only
2	Back up the password to Windows Server Active Directory only

If not specified, this setting defaults to 0 (Disabled).

PasswordAgeDays

This setting controls the length of the password. Supported values are:

- **Minimum**: 1 day (When the backup directory is configured to be Azure Active Directory, the minimum is 7 days.)
- **Maximum**: 365 days

If not specified, this setting defaults to 30 days.

PasswordLength

Use this setting to configure the length of the password of the managed local administrator account. Supported values are:

- **Minimum**: 8 characters
- **Maximum**: 64 characters

If not specified, this setting defaults to 14 characters.

PasswordComplexity

Use this setting to configure the required password complexity of the managed local administrator account.

Value	Description of setting
1	Large letters
2	Large letters + small letters
3	Large letters + small letters + numbers
4	Large letters + small letters + numbers + special characters

If not specified, this setting defaults to 4.

> ⓘ **Important**
>
> Windows supports the lower password complexity settings (1, 2, and 3) only for backward compatibility with legacy Microsoft LAPS. We recommend that you always configure this setting to 4.

PasswordExpirationProtectionEnabled

Use this setting to configure enforcement of maximum password age for the managed local administrator account.

Supported values are either 1 (True) or 0 (False).

If not specified, this setting defaults to 1 (True).

> **Tip**
>
> In legacy Microsoft LAPS mode, this setting defaults to False for backward compatibility.

AdministratorAccountName

Use this setting to configure the name of the managed local administrator account.

If not specified, this setting defaults to managing the built-in local administrator account.

> ⓘ **Important**
>
> Don't specify this setting unless you want to manage an account other than the built-in local administrator account. The local administrator account is automatically identified by its well-known relative identifier (RID).

ADPasswordEncryptionEnabled

Use this setting to enable encryption of passwords in Active Directory.

Supported values are either 1 (True) or 0 (False).

ⓘ **Important**

Enabling this setting requires that your Active Directory domain be running at Domain Functional Level 2016 or later.

ADPasswordEncryptionPrincipal

Use this setting to configure the name or security identifier (SID) of a user or group that can decrypt the password that's stored in Active Directory.

This setting is ignored if the password currently is stored in Azure.

If not specified, only members of the Domain Admins group in the device's domain can decrypt the password.

If specified, the specified user or group can decrypt the password that's stored in Active Directory.

ⓘ **Important**

The string that's stored in this setting must be either an SID in string form or the fully qualified name of a user or group. Valid examples include:

- `S-1-5-21-2127521184-1604012920-1887927527-35197`
- `contoso\LAPSAdmins`
- `lapsadmins@contoso.com`

The principal identified (either by SID or by user or group name) must exist and be resolvable by the device.

This setting is ignored unless ADPasswordEncryptionEnabled is configured to True and all other prerequisites are met.

This setting is ignored when Directory Services Repair Mode (DSRM) account passwords are backed up on a domain controller. In that scenario, this setting always defaults to the Domain Admins group of the domain controller's domain.

ADEncryptedPasswordHistorySize

Use this setting to configure how many previous encrypted passwords are remembered in Active Directory. Supported values are:

- **Minimum** : 0 passwords
- **Maximum**: 12 passwords

If not specified, this setting defaults to 0 passwords (disabled).

> ⓘ **Important**
>
> This setting is ignored unless ADPasswordEncryptionEnabled is configured to True and all other prerequisites are met.
>
> This setting also takes effect on domain controllers that back up their DSRM passwords.

ADBackupDSRMPassword

Use this setting to enable backup of the DSRM account password on Windows Server Active Directory domain controllers.

Supported values are either 1 (True) or 0 (False).

This setting defaults to 0 (False).

> ⓘ **Important**
>
> This setting is ignored unless ADPasswordEncryptionEnabled is configured to True and all other prerequisites are met.

PostAuthenticationResetDelay

Use this setting to specify the amount of time (in hours) to wait after an authentication before executing the specified post-authentication actions (see PostAuthenticationActions). Supported values are:

- **Minimum** : 0 hours (setting this value to 0 disables all post-authentication actions)
- **Maximum**: 24 hours

If not specified, this setting defaults to 24 hours.

PostAuthenticationActions

Use this setting to specify the actions to take upon expiration of the configured grace period (see PostAuthenticationResetDelay).

This setting can have one of the following values:

Value	Name	Actions taken when the grace period expires
1	Reset password	The managed account password is reset.
3	Reset password and sign out	The managed account password is reset and any interactive sign-in sessions that use the managed account are terminated.
5	Reset password and reboot	The managed account password is reset and the managed device is immediately restarted.

If not specified, this setting defaults to 3.

ⓘ **Important**

The allowed post-authentication actions are intended to help limit the amount of time a Windows LAPS password can be used before it's reset. Signing out of the managed account or restarting the device are options that help ensure the time is limited. Abruptly terminating signed-in sessions or restarting the device might result in data loss.

From a security perspective, a malicious user who acquires administrative privileges on a device using a valid Windows LAPS password does have the ultimate ability to prevent or circumvent these mechanisms.

See also

- Windows LAPS CSP
- Microsoft Intune

Next steps

- Use event logs for Windows LAPS
- Use Windows LAPS PowerShell cmdlet
- Windows LAPS schema extensions reference

Use Windows LAPS PowerShell cmdlets

Article • 04/11/2023

Windows Local Administrator Password Solution (Windows LAPS) includes a specific PowerShell module named LAPS. Learn how to use the cmdlets in this module and what they do.

> ⓘ **Important**
>
> For more information on specific OS updates required to use the Windows LAPS feature, and the current status of the Azure Active Directory LAPS scenario, see **Windows LAPS availability and Azure AD LAPS public preview status**.

Cmdlet descriptions

The following table describes the cmdlets that are available in the LAPS PowerShell module:

Name	Description
`Get-LapsAADPassword`	Use to query Azure Active Directory for Windows LAPS passwords.
`Get-LapsDiagnostics`	Use to collect diagnostic information for investigating issues.
`Find-LapsADExtendedRights`	Use to discover which identities have been granted permissions for an Organization Unit (OU) in Windows Server Active Directory.
`Get-LapsADPassword`	Use to query Windows Server Active Directory for Windows LAPS passwords.
`Invoke-LapsPolicyProcessing`	Use to initiate a policy processing cycle.
`Reset-LapsPassword`	Use to initiate an immediate password rotation. Use when backing up the password to either Azure Active Directory or Windows Server Active Directory.
`Set-LapsADAuditing`	Use to configure Windows LAPS-related auditing on OUs in Windows Server Active Directory.
`Set-LapsADComputerSelfPermission`	Use to configure an OU in Windows Server Active Directory to allow computer objects to update their Windows LAPS passwords.

Name	Description
`Set-LapsADPasswordExpirationTime`	Use to update a computer's Windows LAPS password expiration time in Windows Server Active Directory.
`Set-LapsADReadPasswordPermission`	Use to grant permission to read the Windows LAPS password information in Windows Server Active Directory.
`Set-LapsADResetPasswordPermission`	Use to grant permission to update the Windows LAPS password expiration time in Windows Server Active Directory.
`Update-LapsADSchema`	Use to extend the Windows Server Active Directory schema with the Windows LAPS schema attributes.

> **Tip**
>
> - The `Invoke-LapsPolicyProcessing` and `Reset-LapsPassword` cmdlets aren't affected by whether the password currently is backed up to Azure Active Directory or Windows Server Active Directory. In this scenario, both options are supported.
> - All cmdlets in the Windows LAPS PowerShell module support detailed logging when you use the `-Verbose` parameter.

Windows LAPS PowerShell vs. legacy Microsoft LAPS PowerShell

Legacy Microsoft LAPS includes a PowerShell module named AdmPwd.PS. The two modules have many functional similarities, but they also have many differences. This table provides a mapping between the two modules:

Windows LAPS cmdlet	Legacy Microsoft LAPS cmdlet
`Get-LapsAADPassword`	Doesn't apply
`Get-LapsDiagnostics`	Doesn't apply
`Find-LapsADExtendedRights`	`Find-AdmPwdExtendedRights`
`Get-LapsADPassword`	`Get-AdmPwdPassword`
`Invoke-LapsPolicyProcessing`	Doesn't apply
`Reset-LapsPassword`	Doesn't apply

Windows LAPS cmdlet	Legacy Microsoft LAPS cmdlet
`Set-LapsADAuditing`	`Set-AdmPwdAuditing`
`Set-LapsADComputerSelfPermission`	`Set-AdmPwdComputerSelfPermission`
`Set-LapsADPasswordExpirationTime`	`Reset-AdmPwdPassword`
`Set-LapsADReadPasswordPermission`	`Set-AdmPwdReadPasswordPermission`
`Set-LapsADResetPasswordPermission`	`Set-AdmPwdResetPasswordPermission`
`Update-LapsADSchema`	`Update-AdmPwdADSchema`

In addition to naming-related changes, the Windows LAPS PowerShell cmdlets for Windows Server Active Directory operate over an entirely different set of schema extensions. For more information, see Windows LAPS schema extensions reference.

Next steps

- Get started with Windows LAPS in legacy Microsoft LAPS emulation mode
- Use Windows LAPS event logs
- Key concepts in Windows LAPS

Use Windows LAPS event logs

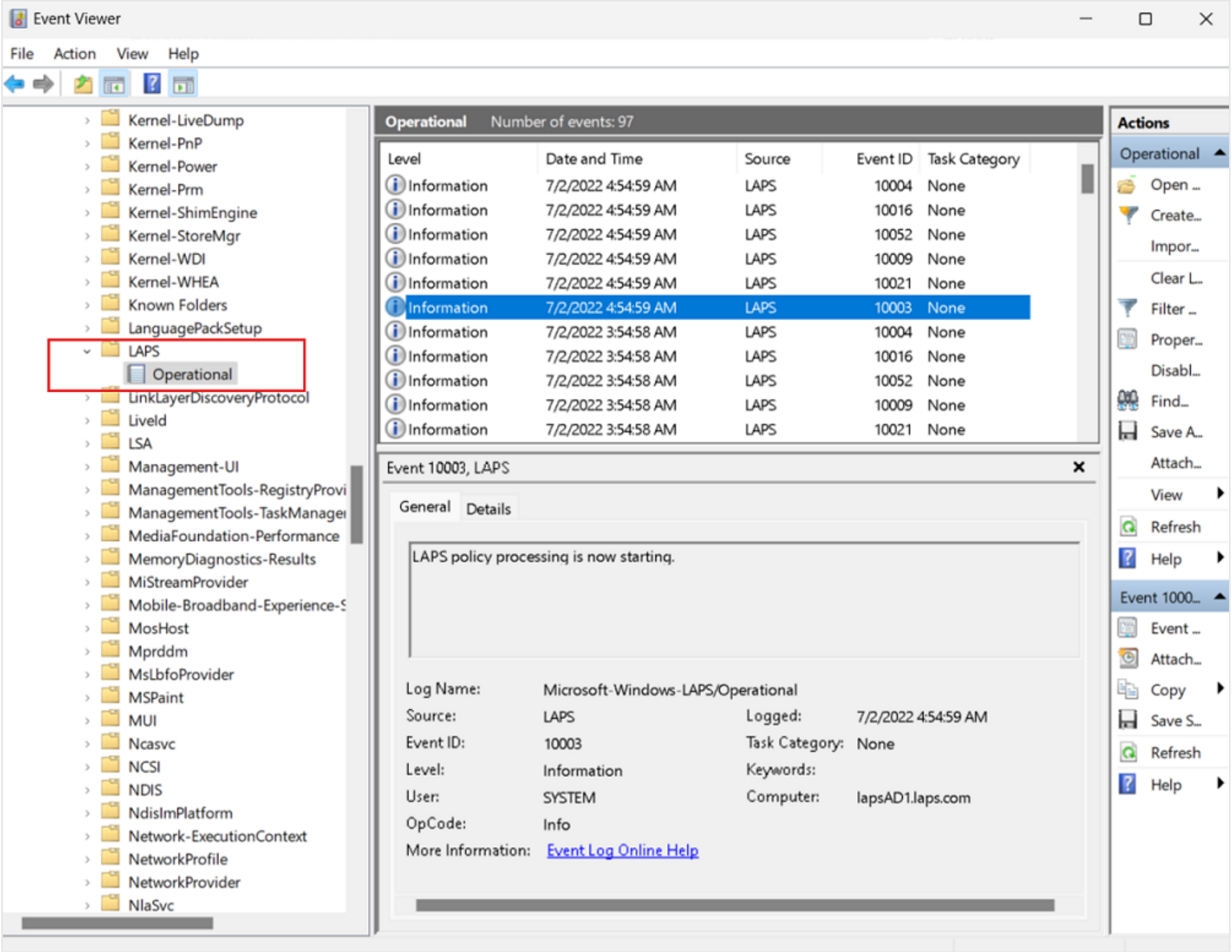
Article • 04/11/2023

Windows Local Administrator Password Solution (Windows LAPS) has a dedicated event log channel. All Windows LAPS operations are tracked with rich eventing. Learn about key events and how to view the log.

> ⓘ **Important**
>
> For more information on specific OS updates required to use the Windows LAPS feature, and the current status of the Azure Active Directory LAPS scenario, see **Windows LAPS availability and Azure AD LAPS public preview status**.

View the event log

To view the Windows LAPS event log channel, in Windows Server Event Viewer, go to **Applications and Services** > **Logs** > **Microsoft** > **Windows** > **LAPS** > **Operational**.



Operational Number of events: 97

Level	Date and Time	Source	Event ID	Task Category
Information	7/2/2022 4:54:59 AM	LAPS	10004	None
Information	7/2/2022 4:54:59 AM	LAPS	10016	None
Information	7/2/2022 4:54:59 AM	LAPS	10052	None
Information	7/2/2022 4:54:59 AM	LAPS	10009	None
Information	7/2/2022 4:54:59 AM	LAPS	10021	None
Information	7/2/2022 4:54:59 AM	LAPS	10003	None
Information	7/2/2022 3:54:58 AM	LAPS	10004	None
Information	7/2/2022 3:54:58 AM	LAPS	10016	None
Information	7/2/2022 3:54:58 AM	LAPS	10052	None
Information	7/2/2022 3:54:58 AM	LAPS	10009	None
Information	7/2/2022 3:54:58 AM	LAPS	10021	None

Event 10003, LAPS

LAPS policy processing is now starting.

Log Name: Microsoft-Windows-LAPS/Operational
Source: LAPS
Logged: 7/2/2022 4:54:59 AM
Event ID: 10003
Task Category: None
Level: Information
Keywords:
User: SYSTEM
Computer: lapsAD1.laps.com
OpCode: Info
More Information: Event Log Online Help

Key events

It's important to be aware of some key Windows LAPS events and how to view them in the event logs:

- Policy processing start and end events
- Policy configuration details
- Password update confirmation events
- Blocked external password modification request
- Post-authentication-action related events

Policy processing cycle start and end

When Windows LAPS begins a background policy processing cycle, the progress of the operation is tracked in the event log. Knowing the specific events that indicate the start and end of each cycle makes it easy to read the event log and understand the events.

Each background policy processing cycle starts with a 10003 event:

Output

```
LAPS policy processing is now starting.
```

Each 10003 event is followed by several other events that describe what's happening. When the cycle finishes, the final event marks the operation as succeeded or failed.

A successful cycle is marked by a 10004 event. Here's an example of a 10004 event:

Output

```
LAPS policy processing succeeded.
```

A failed cycle is marked by a 10005 event. Here's an example of a 10005 event:

Output

```
LAPS policy processing failed with the error code below.

Error code: 80070032
```

If a failure occurs, you can use the error code to troubleshoot. You also can look at the intervening events for detailed information.

Policy configuration details

When password backup is enabled, a policy configuration event is emitted during each Windows LAPS background policy processing cycle. The event logs the specific policy setting value for each cycle iteration.

When the policy is configured to back up the password to Windows Server Active Directory, a 10021 event is logged. Here's an example of a 10021 event:

Output

```
The current LAPS policy is configured as follows:

Policy source: GPO
Backup directory: Active Directory
Local administrator account name:
Password age in days: 30
Password complexity: 4
Password length: 14
Password expiration protection enabled: 1
Password encryption enabled: 1
Password encryption target principal: LapsAdministrators@contoso.com
Password encrypted history size: 12
Backup DSRM password on domain controllers: 0
Post authentication grace period (hours): 8
Post authentication actions: 1
```

When the policy is configured to back up the password to Azure Active Directory, a 10022 event is logged. Here's an example of a 10022 event:

Output

```
The current LAPS policy is configured as follows:

Policy source: CSP
Backup directory: Azure AD
Local administrator account name: ContosoLocalAdminAccount
Password age in days: 7
Password complexity: 4
Password length: 64
Post authentication grace period (hours): 8
Post authentication actions: 3
```

When Windows LAPS is configured to use a legacy Microsoft LAPS policy, a 10023 event is logged. Here's an example of a 10023 event:

Output

```
The current LAPS policy is configured as follows:

Policy source: Legacy LAPS
Backup directory: Active Directory
Local administrator account name:
Password age in days: 30
Password complexity: 4
Password length: 8
Password expiration protection enabled: 0
```

These specific policy setting values are examples and shouldn't be considered recommendations.

Password update confirmation events

When Windows LAPS successfully updates the configured directory (Windows Server Active Directory or Azure Active Directory) with a new password, a success event is logged: 10018 for password updates in Windows Server Active Directory, and 10029 for password updates in Azure Active Directory.

Here's an example of a 10018 event:

Output

```
LAPS successfully updated Active Directory with the new password.
```

Here's an example of a 10029 event:

Output

```
LAPS successfully updated Azure Active Directory with the new password.
```

When the directory is updated with the new password, Windows LAPS also updates the managed local account. A 10020 event is logged on success.

Here's an example of a 10020 event:

Output

```
LAPS successfully updated the local admin account with the new password.

Account name: ContosoLocalAdminAccount
Account RID: 1087
```

Blocked external password modification request

When Windows LAPS is enabled, it protects the password for the specified managed account from being modified by any entity other than Windows LAPS. A 10031 event is logged when an attempt to change the password is blocked.

Here's an example of a 10031 event:

Output

```
LAPS blocked an external request that tried to modify the password of the
current managed account.

Account name: ContosoLocalAdminAccount
Account RID: 1087
```

Post-authentication action events

When post-authentication actions are configured, Windows LAPS monitors for successful authentications by the specified managed account. When an authentication is detected, a 10041 event is logged.

Here's an example of a 10041 event:

Output

```
LAPS detected a successful authentication for the currently managed account.
A background task has been scheduled to execute the configured post-
authentication actions after the configured grace period has expired.%n

Account name: ContosoLocalAdminAccount
Account RID: 1087
Password reset timer deadline: %3%n
```

When the deadline that's listed in the 10031 event is reached, Windows LAPS logs a 10042 event:

Output

```
The post-authentication grace period has expired per policy. The configured
post-authentication actions will now be executed.

Account name: ContosoLocalAdminAccount
Account RID: 1087
```

Windows LAPS then attempts to rotate the password and execute any specified post-authentication actions. A 10044 event is logged when the password rotation succeeds.

Here's an example of a 10044 event:

Output

```
LAPS successfully reset the password for the currently managed account and
completed all configured post-authentication actions.%n
%n
Account name: ContosoLocalAdminAccount
Account RID: 1087
```

If the password rotation fails, a 10043 event is logged. Here's an example of a 10043 event:

Output

```
LAPS failed to reset the password for the currently managed account. The
password is considered expired due to an authentication event. LAPS will
continue retrying the password reset operation until it succeeds.

Account name: ContosoLocalAdminAccount
Account RID: 1087
Password reset retry count: 1
Error code: 80070032
```

Next steps

- Configure Windows LAPS for Windows Server Active Directory
- Key concepts in Windows LAPS

Set up Windows LAPS in the LAPS properties dialog

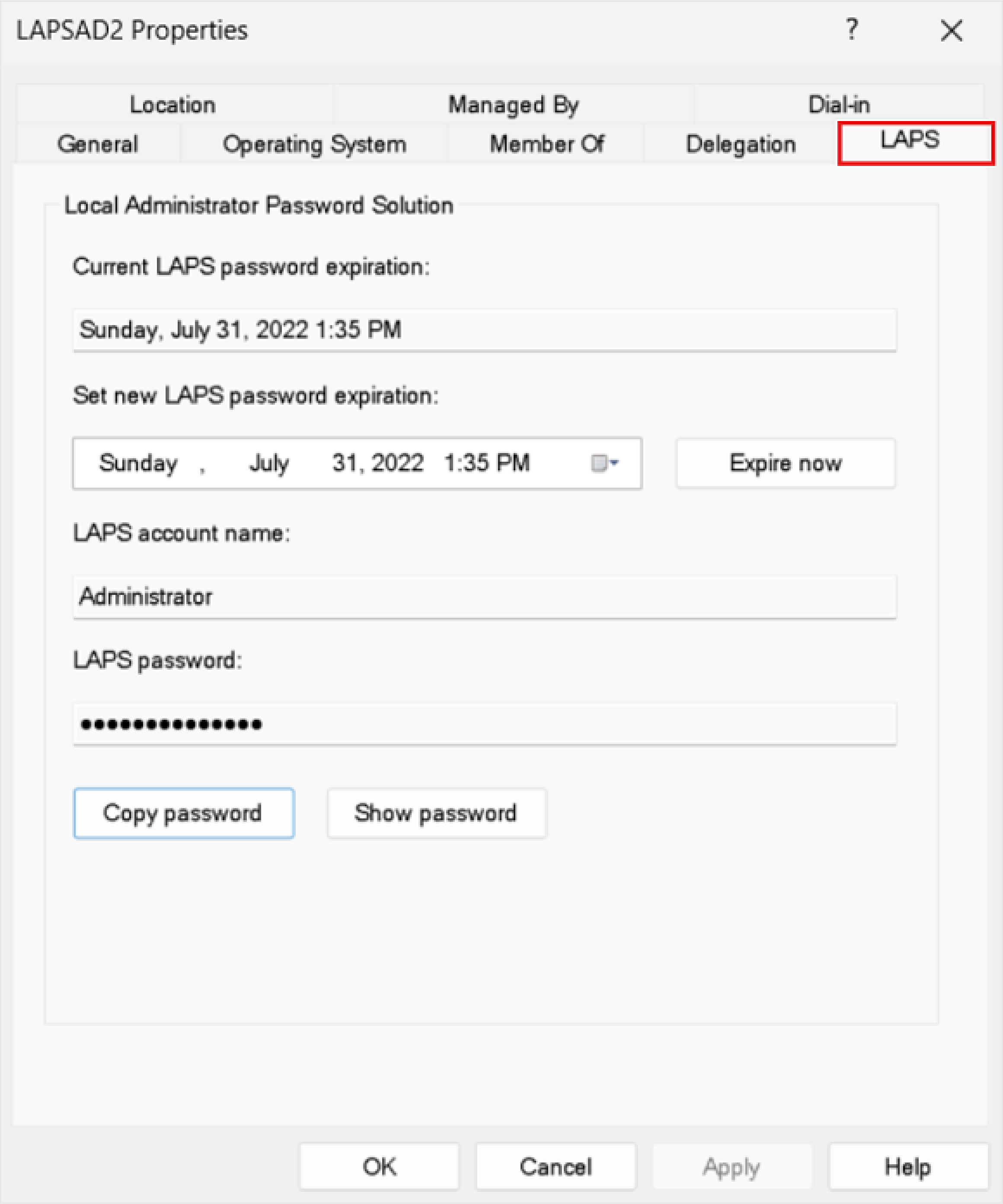
Article • 04/11/2023

Learn how to use the LAPS properties dialog in the Windows Server Active Directory Users and Computers management snap-in to configure Windows Local Administrator Password Solution (Windows LAPS) for Windows Server Active Directory.

> ⓘ **Important**
>
> For more information on specific OS updates required to use the Windows LAPS feature, and the current status of the Azure Active Directory LAPS scenario, see **Windows LAPS availability and Azure AD LAPS public preview status**.

LAPS properties dialog in the management snap-in

The Windows Server Active Directory Users and Computers management snap-in includes a LAPS properties dialog that's available for computer objects:



Local Administrator Password Solution

Current LAPS password expiration:

Sunday, July 31, 2022 1:35 PM

Set new LAPS password expiration:

Sunday , July 31, 2022 1:35 PM

LAPS account name:

Administrator

LAPS password:

●●●●●●●●●●●●●●

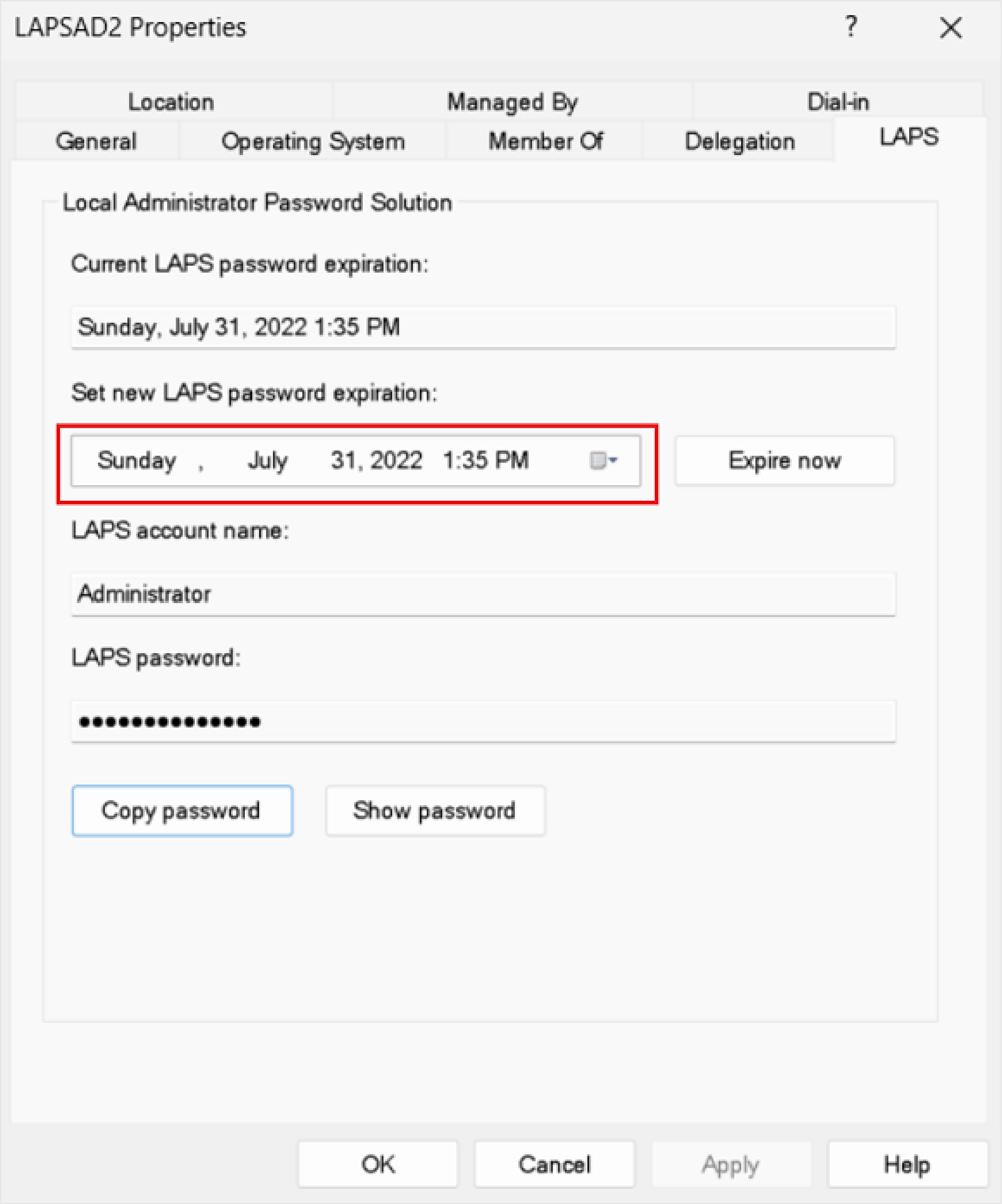
You can use the properties dialog to complete the following actions:

- View the current password expiration time.
- Modify the password expiration time.
- Expire the password expiration time.
- View the current account name and password.

> ⓘ **Important**
>
> The LAPS properties dialog doesn't support viewing legacy Microsoft LAPS passwords or password expiration times.

View the current password expiration time

When you first go to the properties dialog for a Windows Server Active Directory computer, the date-time control displays the current password expiration time. For example:



LAPSAD2 Properties

Local Administrator Password Solution

Current LAPS password expiration: Sunday, July 31, 2022 1:35 PM

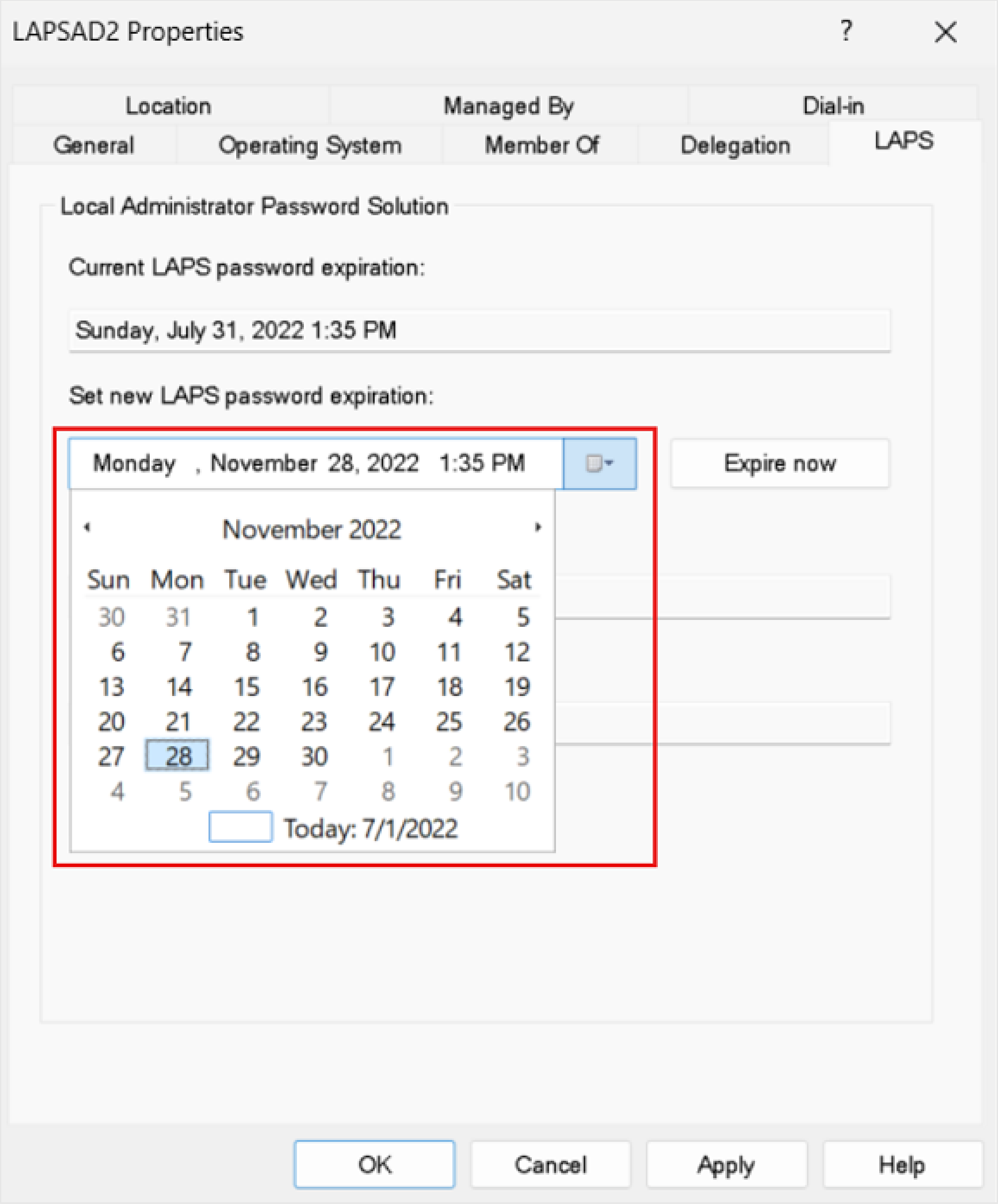
Set new LAPS password expiration: Sunday , July 31, 2022 1:35 PM

LAPS account name: Administrator

LAPS password: •••••••••••••••

Modify the password expiration time

You can use the date-time control to modify the password expiration time. For example:



Local Administrator Password Solution

Current LAPS password expiration:

Sunday, July 31, 2022 1:35 PM

Set new LAPS password expiration:

Monday , November 28, 2022 1:35 PM

November 2022

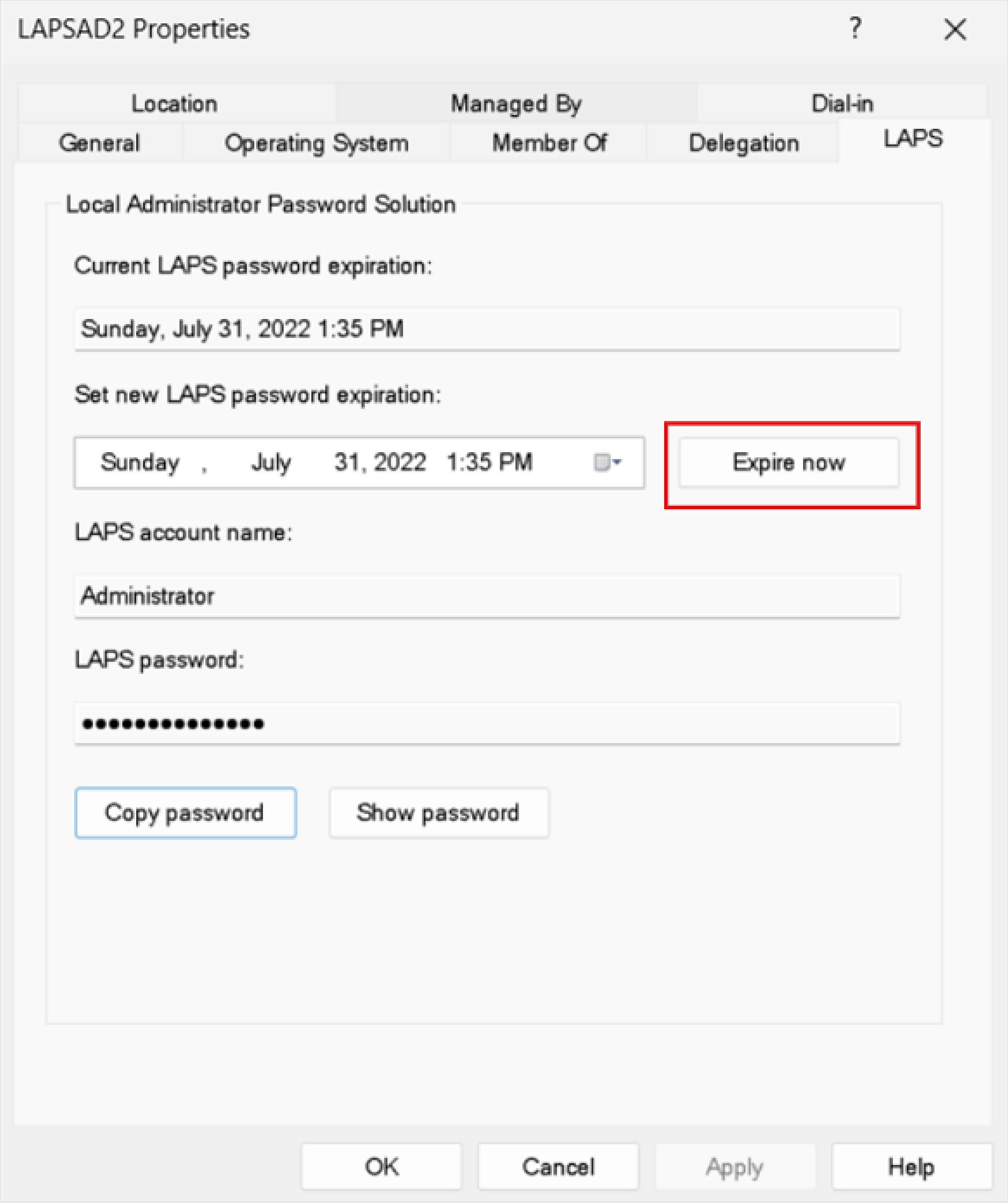
Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Today: 7/1/2022

If you modify the date or time, select **Apply**, and then select **OK**.

Manually expire the password

To immediately expire the password, select **Expire now**:



LAPSAD2 Properties

Local Administrator Password Solution

Current LAPS password expiration:

Sunday, July 31, 2022 1:35 PM

Set new LAPS password expiration:

Sunday , July 31, 2022 1:35 PM

LAPS account name:

Administrator

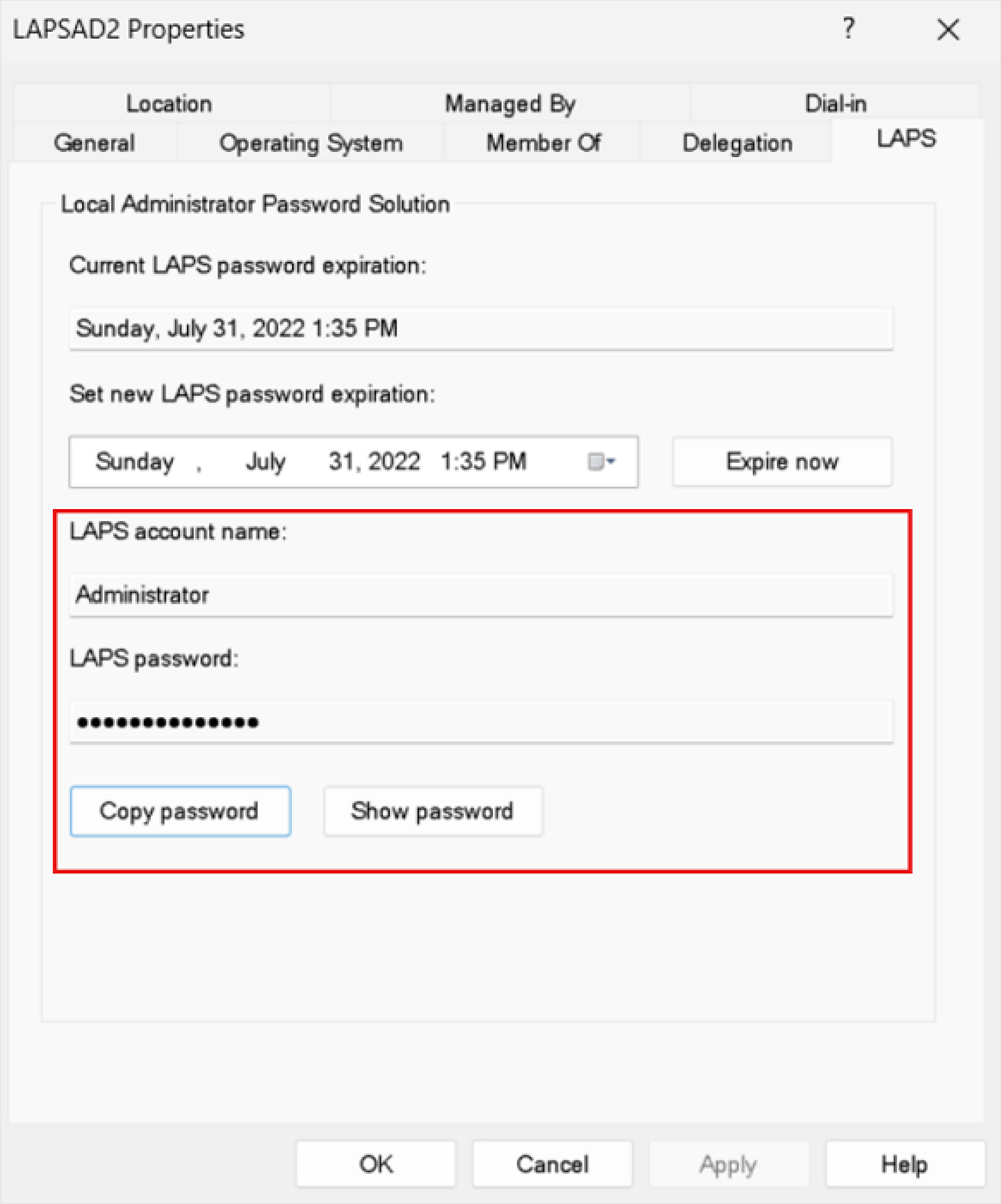
LAPS password:

●●●●●●●●●●●●●●●

Select **Apply**, and then select **OK**.

View the current account name and password

If you have permissions to read and decrypt the computer's current Windows LAPS password attribute, **Account Name** and **Password** have your username and password. Select **Copy password** to copy the password to the clipboard. Select **Show password** to show the password.


LAPSAD2 Properties

Location | Managed By | Dial-in | General | Operating System | Member Of | Delegation | LAPS

Local Administrator Password Solution

Current LAPS password expiration:

Sunday, July 31, 2022 1:35 PM

Set new LAPS password expiration:

Sunday , July 31, 2022 1:35 PM

LAPS account name:

Administrator

LAPS password:

•••••••••••••••

If you don't have permissions to read or decrypt the current password information, a dialog displays a warning.

ⓘ **Important**

The Active Directory Users and Computers management snap-in only supports viewing the most recently stored password. In order to query older passwords (assuming you enabled password history), you must use the `Get-LapsADPassword` PowerShell cmdlet.

Next steps

- Windows LAPS schema extensions reference
- Key concepts in Windows LAPS

Windows LAPS schema extensions reference

Article • 04/11/2023

Use detailed information about schema extensions and extended rights to help you deploy or manage Windows Local Administrator Password Solution (Windows LAPS) in your Windows Server Active Directory deployment.

ⓘ **Important**

For more information on specific OS updates required to use the Windows LAPS feature, and the current status of the Azure Active Directory LAPS scenario, see **Windows LAPS availability and Azure AD LAPS public preview status**.

Schema extensions

Windows LAPS offers specific schema elements for Windows Server Active Directory. To use any of the following Windows LAPS Windows Server Active Directory-based features, you must add these new schema elements to the forest by running the `Update-LapsADSchema PowerShell` cmdlet.

Schema attributes

Windows LAPS uses specific schema attributes that are stored on the computer object in Windows Server Active Directory for a managed device. The `Update-LapsADSchema` cmdlet adds the schema attributes to the directory and to the `mayContain` list on the computer schema class.

Tip

Many of the following attributes specify a `SearchFlags` value of `904`. For easy reference, this value is composed of the following bit flags:

- `fRODCFilteredAttribute`
- `fNEVERVALUEAUDIT`
- `fCONFIDENTIAL`
- `fPRESERVEONDELETE`

msLAPS-PasswordExpirationTime

This attribute contains a 64-bit integer that specifies the currently scheduled password expiration time in UTC.

PowerShell

```
Name: ms-LAPS-PasswordExpirationTime
LDAP display name: msLAPS-PasswordExpirationTime
OID: 1.2.840.113556.1.6.44.1.1
Syntax: 2.5.5.16
OmSyntax: 65
IsSingleValued: True
IsMemberOfPartialAttributeSet: False
SearchFlags: 0
AttributeSecurityGuid: <not set>
```

msLAPS-Password

This attribute contains a Unicode string that specifies the clear-text version of the current password and other information.

PowerShell

```
Name: ms-LAPS-Password
LDAP display name: msLAPS-Password
OID: 1.2.840.113556.1.6.44.1.2
Syntax: 2.5.5.5
OmSyntax: 19
IsSingleValued: True
IsMemberOfPartialAttributeSet: False
SearchFlags: 904
AttributeSecurityGuid: <not set>
```

The data that's stored in this attribute is a JSON string that contains multiple name-value pairs. For example:

```
{"n":"Administrator","t":"1d8161b41c41cde","p":"A6a3#7%eb!57be4a4B95Z43394ba956de69e5d8975#$8a6d)4f82da6ad500HGx"}
```

Each name-value pair in the JSON string has a specific meaning:

Name	Value
`"n"`	Contains the name of the managed local administrator account

Name	Value
`"t"`	Contains the UTC password update time represented as a 64-bit hexadecimal number
`"p"`	Contains the clear-text password

msLAPS-EncryptedPassword

This attribute contains a byte string that contains an encrypted version of the current password.

PowerShell

```PowerShell
Name: ms-LAPS-EncryptedPassword
LDAP display name: msLAPS-EncryptedPassword
OID: 1.2.840.113556.1.6.44.1.3
Syntax: 2.5.5.10
OmSyntax: 4
IsSingleValued: True
IsMemberOfPartialAttributeSet: False
SearchFlags: 904
AttributeSecurityGuid: f3531ec6-6330-4f8e-8d39-7a671fbac605 (ms-LAPS-Encrypted-Password-Attributes)
```

msLAPS-EncryptedPasswordHistory

This attribute contains a multi-valued byte string. Each value contains an encrypted version of an earlier password.

PowerShell

```PowerShell
Name: ms-LAPS-EncryptedPasswordHistory
LDAP display name: msLAPS-EncryptedPasswordHistory
OID: 1.2.840.113556.1.6.44.1.4
Syntax: 2.5.5.10
OmSyntax: 4
IsSingleValued: False
IsMemberOfPartialAttributeSet: False
SearchFlags: 904
AttributeSecurityGuid: f3531ec6-6330-4f8e-8d39-7a671fbac605 (ms-LAPS-Encrypted-Password-Attributes)
```

msLAPS-EncryptedDSRMPassword

This attribute contains a byte string that contains an encrypted version of the current Directory Services Restore Mode (DSRM) account password.

PowerShell

```
Name: ms-LAPS-EncryptedDSRMPassword
LDAP display name: msLAPS-EncryptedDSRMPassword
OID: 1.2.840.113556.1.6.44.1.5
Syntax: 2.5.5.10
OmSyntax: 4
IsSingleValued: True
IsMemberOfPartialAttributeSet: False
SearchFlags: 904
AttributeSecurityGuid: f3531ec6-6330-4f8e-8d39-7a671fbac605 (ms-LAPS-
Encrypted-Password-Attributes)
```

msLAPS-EncryptedDSRMPasswordHistory

This attribute contains a multi-valued byte string. Each value contains an encrypted version of an earlier DSRM account password.

PowerShell

```
Name: ms-LAPS-EncryptedDSRMPasswordHistory
LDAP display name: msLAPS-EncryptedDSRMPasswordHistory
OID: 1.2.840.113556.1.6.44.1.6
Syntax: 2.5.5.10
OmSyntax: 4
IsSingleValued: False
IsMemberOfPartialAttributeSet: False
SearchFlags: 904
AttributeSecurityGuid: f3531ec6-6330-4f8e-8d39-7a671fbac605 (ms-LAPS-
Encrypted-Password-Attributes)
```

Extended rights

Windows LAPS extends the `ms-LAPS-Encrypted-Password-Attributes` rights in Windows Server Active Directory. You can use the `ms-LAPS-Encrypted-Password-Attributes` extended rights to grant managed devices SELF permissions to read and write the encrypted password attributes that are described in the preceding sections.

PowerShell

```
Name: ms-LAPS-Encrypted-Password-Attributes
Rights guid: f3531ec6-6330-4f8e-8d39-7a671fbac605
Valid accesses: 48 (RIGHT_DS_READ_PROPERTY | RIGHT_DS_WRITE_PROPERTY)
```

Windows LAPS schema vs. legacy Microsoft LAPS schema

Like Windows LAPS, legacy Microsoft LAPS also requires you to use schema extensions for a Windows Server Active Directory deployment. To help you plan a migration from legacy Microsoft LAPS to Windows LAPS, the following table shows a logical mapping of schema extension elements:

Windows LAPS schema element	Legacy Microsoft LAPS schema element
`msLAPS-PasswordExpirationTime`	`ms-Mcs-AdmPwdExpirationTime`
`msLAPS-Password`	`ms-Mcs-AdmPwd`
`msLAPS-EncryptedPassword`	Doesn't apply
`msLAPS-EncryptedPasswordHistory`	Doesn't apply
`msLAPS-EncryptedDSRMPassword`	Doesn't apply
`msLAPS-EncryptedDSRMPasswordHistory`	Doesn't apply
`ms-LAPS-Encrypted-Password-Attributes`	Doesn't apply

Next steps

- Key concepts in Windows LAPS
- Use Windows LAPS event logs