Windows LAPS (Local Administrator Password Solution)

1. Update Windows Server

Windows LAPS requires at least Windows Server 2019 with a domain functional level of 2016. Be sure to run Windows Update on all Domain Controllers. If you only update 1x Domain Controller and extend the Active Directory schema (next step), it will throw an error. Minimum update level: April 11 2023 Update

2. Extend Active Directory Schema

There is no Windows LAPS client to download and install on the Domain Controller like we are used to with Microsoft LAPS because it's already integrated into Windows Server 2019 and higher.

1. Run PowerShell as administrator on the Domain Controller.

2. Run **ipmo LAPS** to import the LAPS module.

3. Run the **gcm -Module LAPS** command to verify the LAPS module is loaded.

Note: If there is no output after running above command, you must update your Windows Server to the supported version (see above).

4. Run the **Update-LapsADSchema** cmdlet, press A, and follow with Enter.

3. Check LAPS attributes

To verify that the LapsAdSchema ran successfully, run the **Update-LapsAdSchema -Verbose**

The end of the output is important, which shows that the LAPS schema is already extended successfully with the attributes:

msLAPS-PasswordExpirationTime

msLAPS-Password

msLAPS-EncryptedPassword

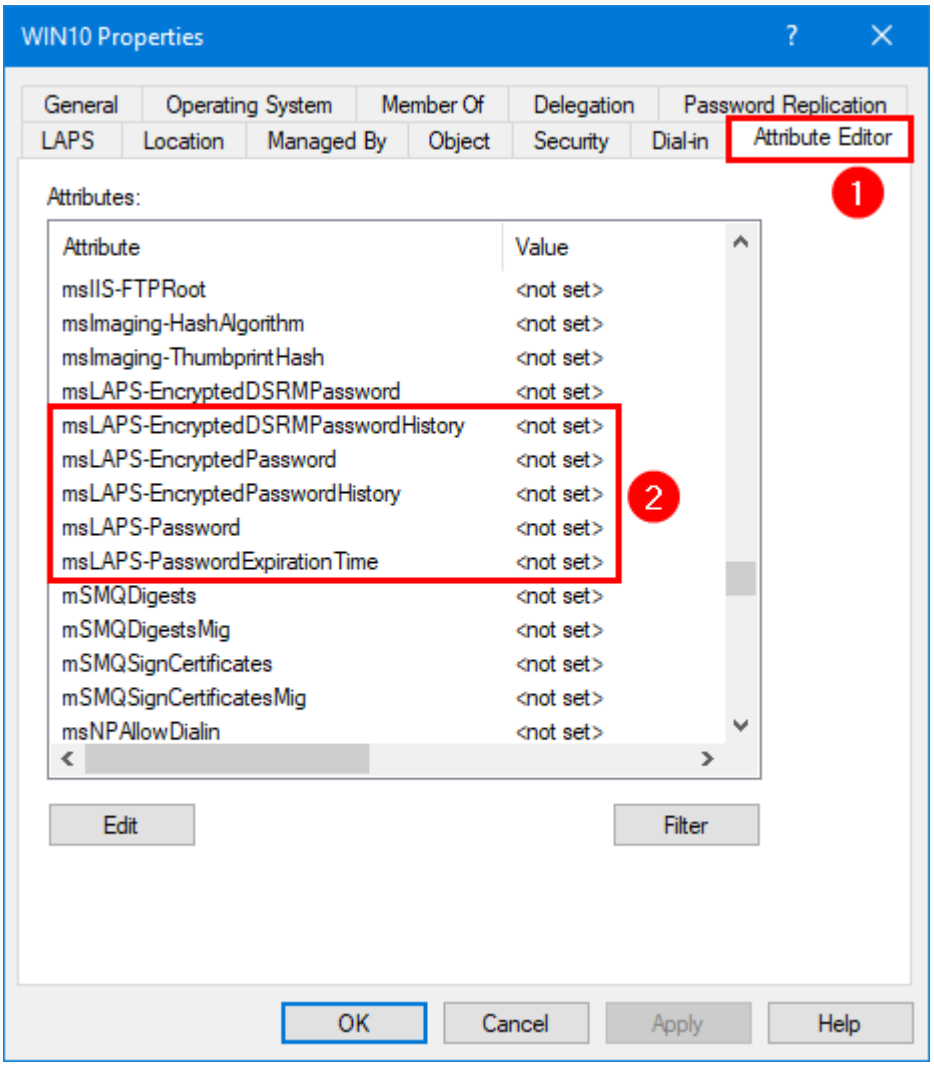
msLAPS-EncryptedPasswordHistory

msLAPS-EncryptedDSRMPassword

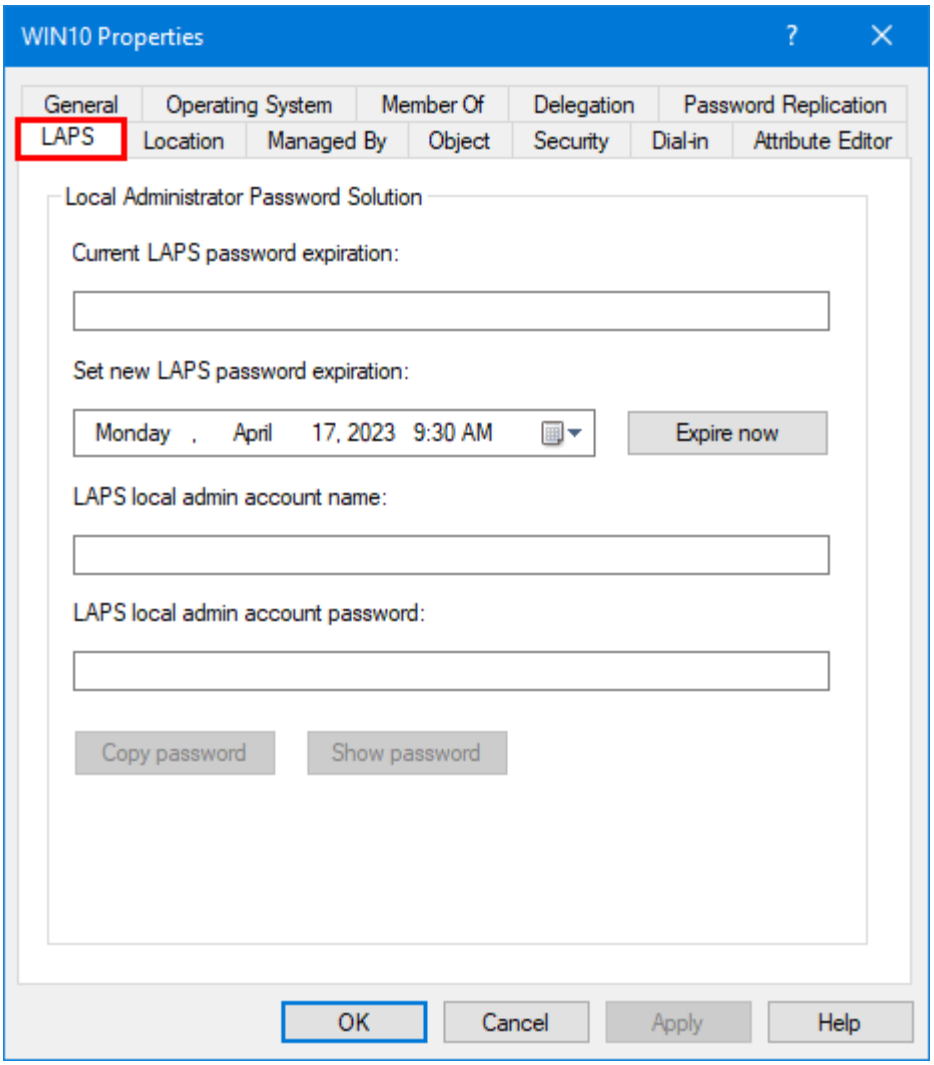
msLAPS-EncryptedDSRMPasswordHistory

Go to a Windows 10/Windows 11 AD object properties and select the Attribute tab.

Note: If you don't see the Attribute Editor tab, click in Active Directory Users and Computers in the menu bar on View and enable Advanced Features.



You will also see the LAPS tab, and you can click on it. But it's empty for now and will populate information once you complete all the steps.



4. Set LAPS AD Computer permission

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 setting will apply to all nested OUs too. In this example we will set the permissions for our 'Workstations' OU.

PS C:\> **Set-LapsADComputerSelfPermission -Identity "OU=Workstations,DC=school,DC=local"**

5. Set up LAPS GPO

Configure a GPO for LAPS and enable its settings.

1. Start Group Policy Management on the Domain Controller.

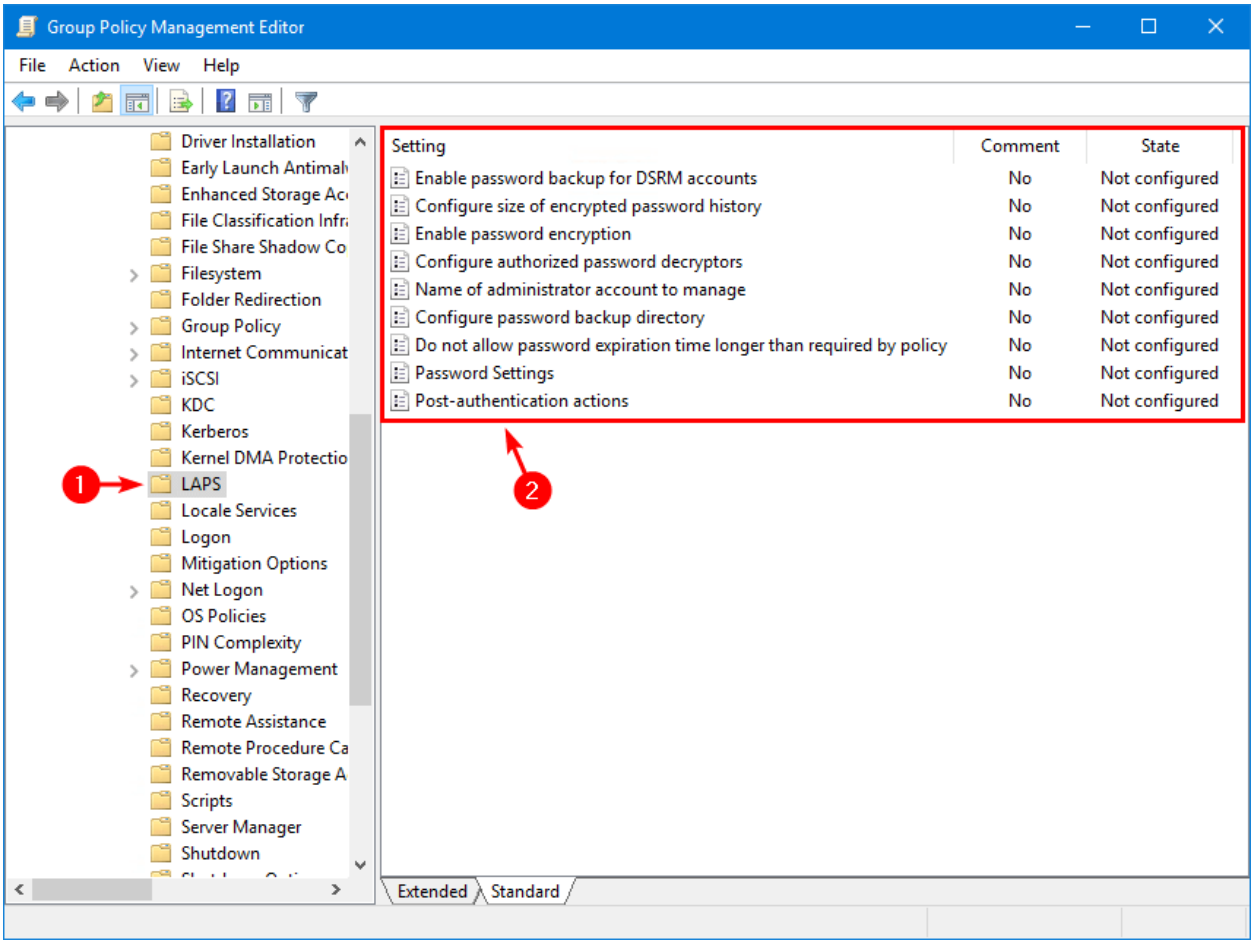
2. Right-click the Workstations OU.

3. Click Create a GPO in this domain, and link it here.

4. Give the Policy the name: **LAPS**

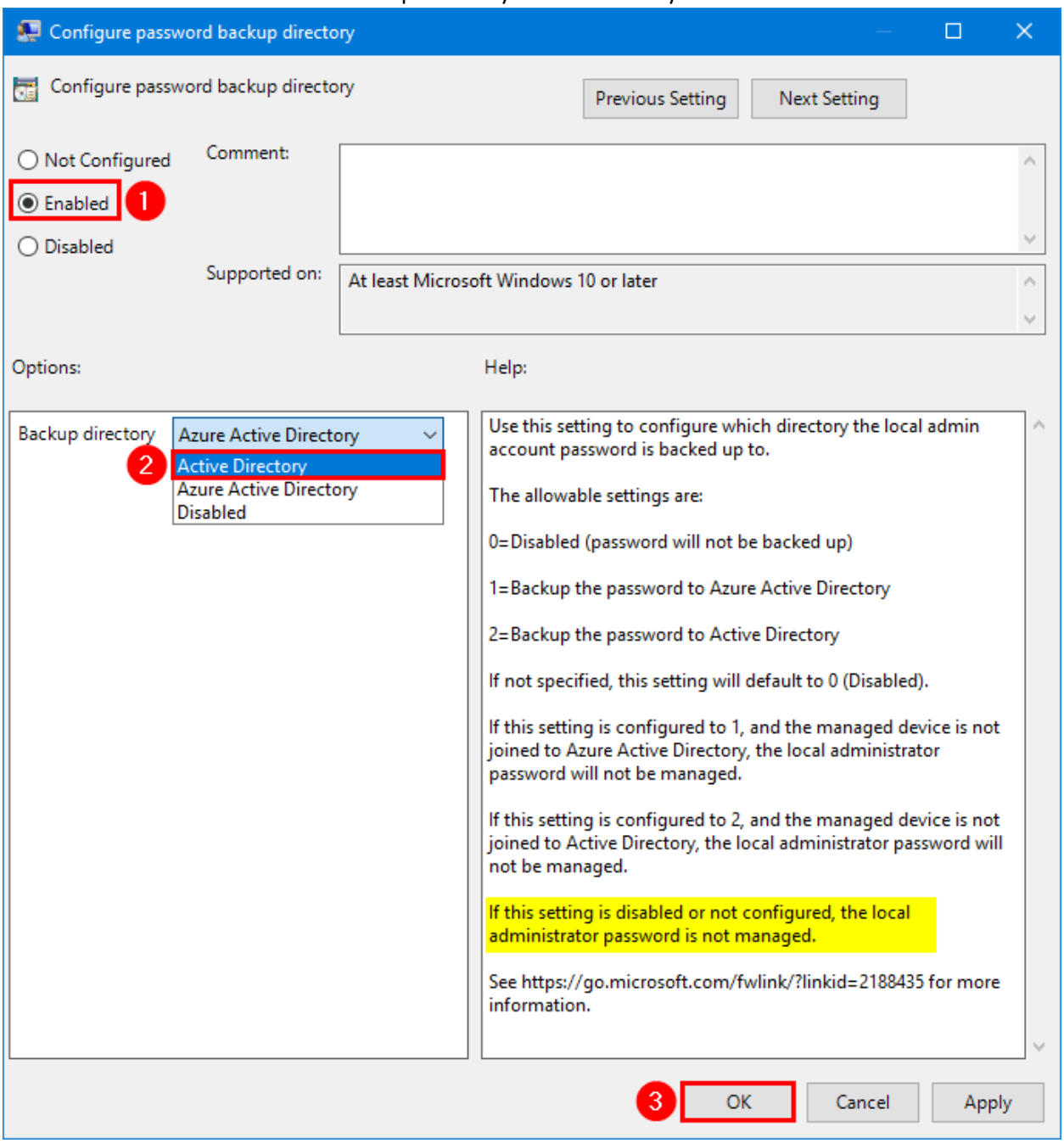
5. Right-click the **LAPS** GPO and click Edit.

6. Navigate to **Computer Configuration > Policies > Administrative Templates > System > LAPS**.



7. Double-click on Configure password backup directory setting.

8. Select Enabled and choose the backup directory Active Directory.

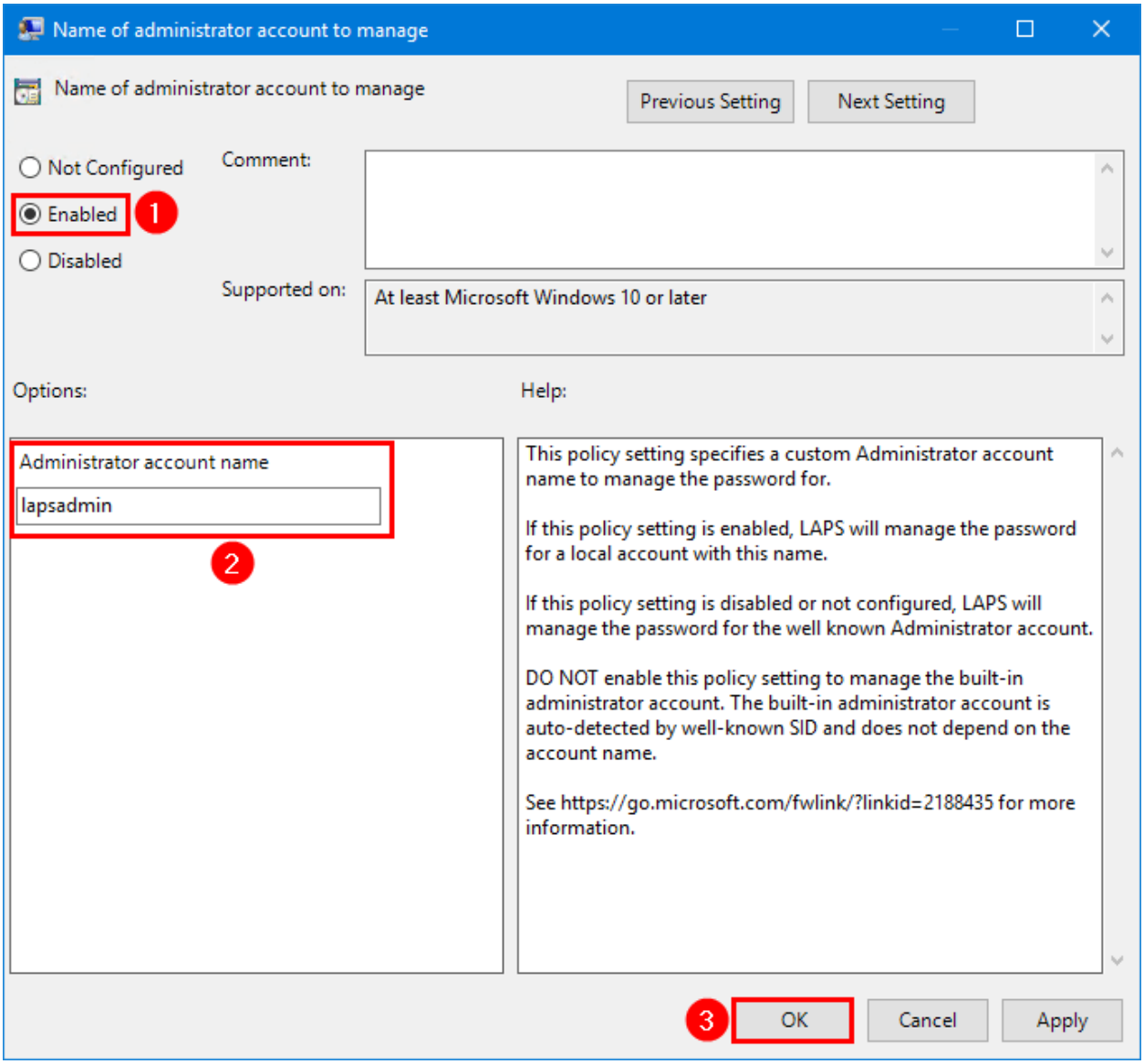


9. Double-click on Password Settings setting.

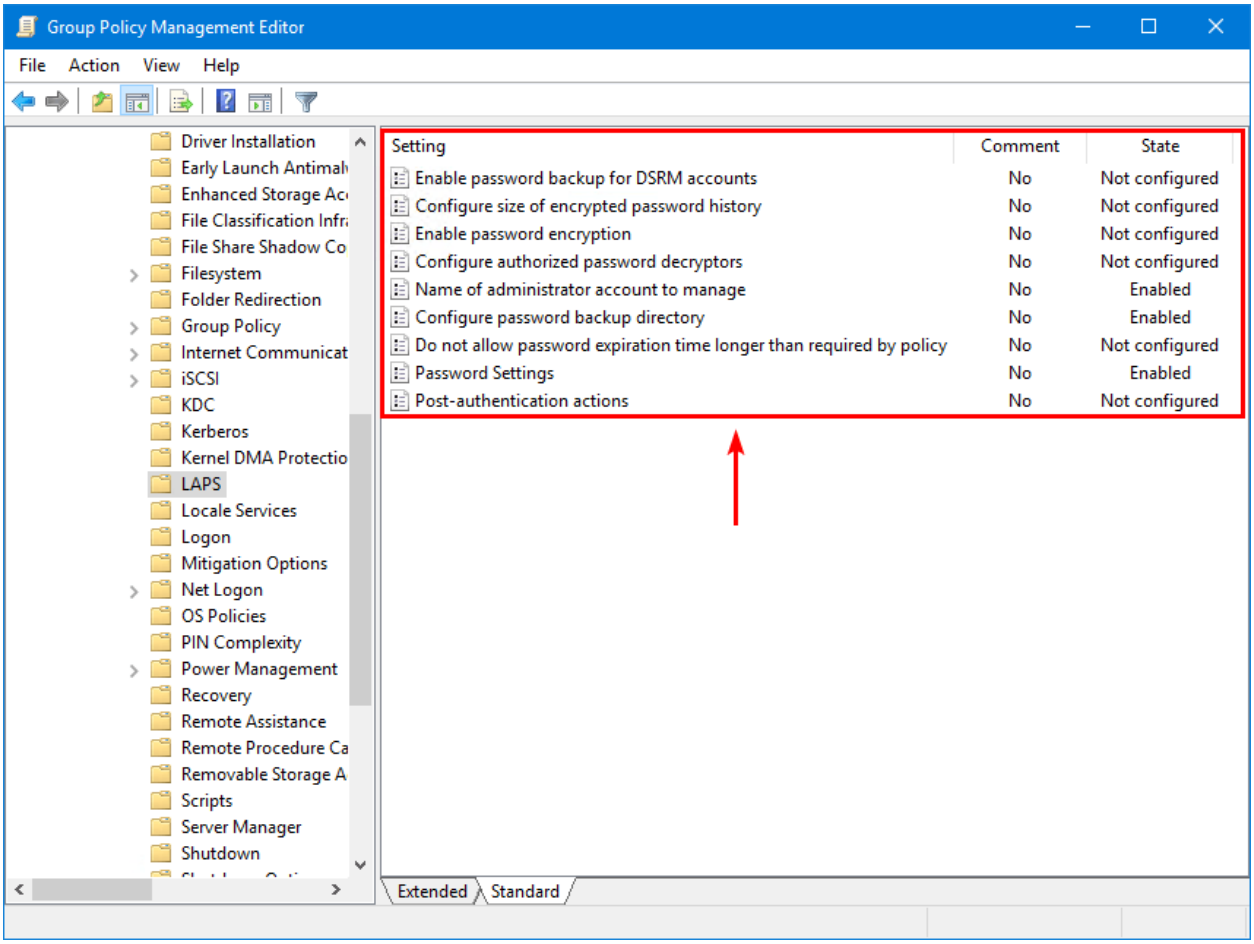
10. Select Enabled and configure the password complexity.

11. ***IF*** you are managing the password for an account other than the built-in local Administrator; Double-click on Name of administrator account to manage setting.

12. Select Enabled and insert the administrator account name **lapsadmin**.



13. This is what the LAPS GPO state looks like.



6. Create local admin account

In the previous step, we did enable the Name of administrator account to manage setting and set the administrator account name: **lapsadmin**.

The LAPS GPO will not create your local administrator account on all the machines. That's something you have to take care of with another GPO, a PowerShell script, or another choice.

***Important**: Disable all the other local admin accounts and ensure that only the lapsadmin account is enabled for security purposes.*

7. Get LAPS password

Now let's see how to retrieve the LAPS Password in GUI.

Get the LAPS password directly from the Active Directory Users and Computer console.

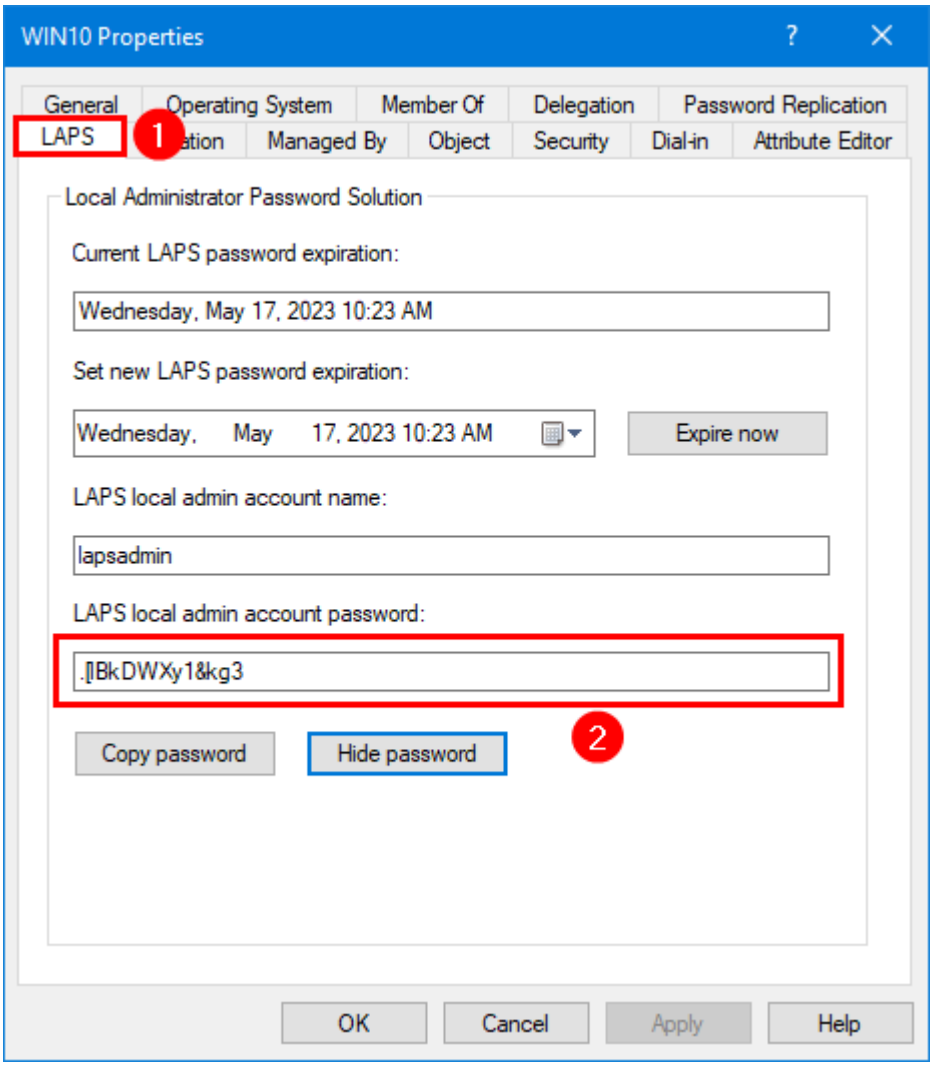
1. Start Active Directory Users and Computers.

2. Go to the AD computer object properties.

3. Select the tab LAPS.

You will see that the fields are now filled in and are not empty anyme. It means that Active Directory connected with the Windows computer and synchronized the information.

4. Click on Show Password.



8. Get LAPS password from PowerShell

1. Open powershell as administrator

2. Run **Get-LapsADPassword -Identity *ComputerName* -AsPlainText**