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.

IN10 Pro	perties							?	×
General	Operatin	g System	Me	mber Of	Delegatio	n Pas	swor	d Repli	cation
LAPS	Location	Managed	By	Object	Security	Dial-in	A	ttribute	Editor
Attributes	:								0
Attribute	,				Value		^		-
msIIS-F	TPRoot				<not set=""></not>				
msImag	ing-HashAlg	orithm			<not set=""></not>				
msImag	ing-Thumbo	rintHash			<not set=""></not>				
msLAPS	6-Encrypted	DSRMPass	word		<not set=""></not>				
msLAPS	6-Encrypted	DSRMPass	wordH	listory	<not set=""></not>				
msLAPS	5-Encrypted	Password			<not set=""></not>				
msLAPS	5-Encrypted	PasswordHi	istory		<not set=""></not>	2			
msLAPS	S-Password				<not set=""></not>	•			
msLAPS	S-Password	Expiration Tir	ne		<not set=""></not>				
mSMQE	Digests				<not set=""></not>				
mSMQE	DigestsMig				<not set=""></not>				
mSMQS	SignCertificat	tes			<not set=""></not>				
mSMQS	SignCertificat	tesMig			<not set=""></not>				
msNPA	lowDialin				<not set=""></not>		×		
<						>			
E 15						F * b			
Edi						Filter			
			V			Arrely			1-1-

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.

VIN10 Pro	perties						?	×
General	Operatin	g System	Me	ember Of	Delegation	Pass	word Replic	ation
LAPS	Location	Managed	By	Object	Security	Dial-in	Attribute	Editor
Curren	Administrator It LAPS pase	Password S	Solution:	n				
Set ne	w LAPS pas	pril 17, 2	ation:	9:30 AM		Expire	now	
LAPS	local admin	account na	me:					
LAPS	local admin	account pa	sswor	d:				
		_	_					
Coj	py password	l Sh	iow pa	assword				
		0	К	Ca	ncel	Apply	He	elp

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**.

Note: If you don't see LAPS and you manage a Central Store for your Policy Definitions, you will have to copy the latest ADMX and ADML files from C:\Windows\PolicyDefinitions (Particularly the LAPS.ADMX and LAPS.ADML files.



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

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

💭 Configure passw	ord backup directo	ry			—		×
Configure password backup directory Previous Setting Next Setting							
O Not Configured	Comment:						^
 Disabled 	Supported on:						~
	Supported on.	At least Microso	oft Windows	10 or later			$\hat{}$
Options:			Help:				
Backup directory	Azure Active Directo Active Directory	ory ~	Use this set account pa	ting to configure wh ssword is backed up	ich directory the lo to.	cal admin	^
	Azure Active Directo Disabled	iry	The allowa	ble settings are:			
			0=Disabled	(password will not b	e backed up)		
			1=Backup t	the password to Azur	e Active Directory		
			2=Backup t	the password to Activ	ve Directory		
			If not speci	fied, this setting will	default to 0 (Disable	ed).	
			If this settin joined to A password v	ng is configured to 1, zure Active Directory vill not be managed.	and the managed o , the local administ	device is not rator	:
			If this settir joined to A not be mar	ng is configured to 2, ctive Directory, the lo naged.	and the managed o ocal administrator p	device is not assword wil	
	1=Backup the password to Azure Active Directory 2=Backup the password to Active Directory If not specified, this setting will default to 0 (Disabled). If this setting is configured to 1, and the managed device is not joined to Azure Active Directory, the local administrator password will not be managed. If this setting is configured to 2, and the managed device is not joined to Active Directory, the local administrator password will not be managed. If this setting is disabled or not configured, the local administrator password will not be managed. See https://go.microsoft.com/fwlink/?linkid=2188435 for more						
			See https:// information	/go.microsoft.com/fi n.	wlink/?linkid=21884	135 for more	
							~
				3 01	K Cancel	Арр	ly

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; Doubleclick on Name of administrator account to manage setting. 12. Select Enabled and insert the administrator account name lapsadmin.

👰 Name of adminis	trator account to r	manage			—		×
Name of adminis	trator account to r	nanage	[Previous Setting	Next Setting		
O Not Configured	Comment:						^
O Disabled	Supported on:	At least Microsoft	Windows 1	0 or later			Ŷ
Options:		Н	elp:				
Administrator accour lapsadmin	2	T n lf fc n D a a a S ir	his policy s hame to ma f this policy or a local and f this policy nanage the OO NOT ena dministrate uto-detect ccount nar de https://g nformation	setting specifies a cus nage the password for setting is enabled, L ccount with this nam setting is disabled of password for the we able this policy setting or account. The built- ed by well-known SIE me. go.microsoft.com/fw	stom Administrator ; or. APS will manage the le. r not configured, LA Il known Administra g to manage the bui -in administrator acc) and does not depe /link/?linkid=218843	account e password PS will itor accoun ilt-in count is ind on the 5 for more	t. ~
				3 ок	Cancel	Appl	у

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.

WIN10 Prop	oerties						?	×
General	Operating	g System	Membe	er Of	Delegation	Pass	word Replic	ation
LAPS	ation	Managed	By O	bject	Security	Dial-in	Attribute	Editor
-Local Ac	dministrator LAPS pass	Password \$	Solution — ation:					
Wedne	esday, May	17, 2023 1	0:23 AM					
Set nev	v LAPS pas	sword expi	ration:					
Wedne	sday, M	ay 17,2	2023 10:2	3 AM		Expire	now	
lapsade LAPS lo	min min min admin a	account na	me: ssword:					
.[IBkD\	NXy1&kg3							
Copy	y password	Н	ide passw	ord	2			
		0	К	Can	cel	Apply	He	elp

- 8. Get LAPS password from PowerShell
- 1. Open powershell as administrator
- 2. Run Get-LapsADPassword -Identity ComputerName -AsPlainText