How to install and configure LAPS (Local Administrator Password Solution)

In this post, I will show you how to install, configure and deploy LAPS on Windows Server 2016. I will be installing LAPS on Domain Controller.

I have downloaded the files from Microsoft site. The download link is as follows:

https://www.microsoft.com/en-us/download/details.aspx?id=46899

Local Administrator Password Solution

The "Local Administrator Password Solution" (LAPS) provides a centralized storage of secrets/passwords in Active Directory (AD) - without additional computers. Each organization's domain administrators determine which users, such as helpdesk admins, are authorized to read the passwords.

For occasions when login is required without domain credentials, password management can become complex. LAPS simplify password management while helping customers implement recommended defenses against cyberattacks. In particular, it mitigates the risk of lateral escalation that results when customers have the same administrative local account and password combination on many computers.

Why use LAPS instead of other password managers/vaults?

Other password managers typically require either, additional hardware (IIS/SQL), trusting a third party, or ad hoc practices (Excel spreadsheet of passwords = huge security hole).

LAPS provide a streamlined approach to:

Periodically randomizing local administrator passwords - ensures password update to AD succeeds before modifying local secrets/passwords

Centrally store secrets in existing infrastructure - Active Directory (AD)
Control access via AD ACL permissions
Transmit encrypted passwords from client to AD (using Kerberos encryption, AES cypher by default)

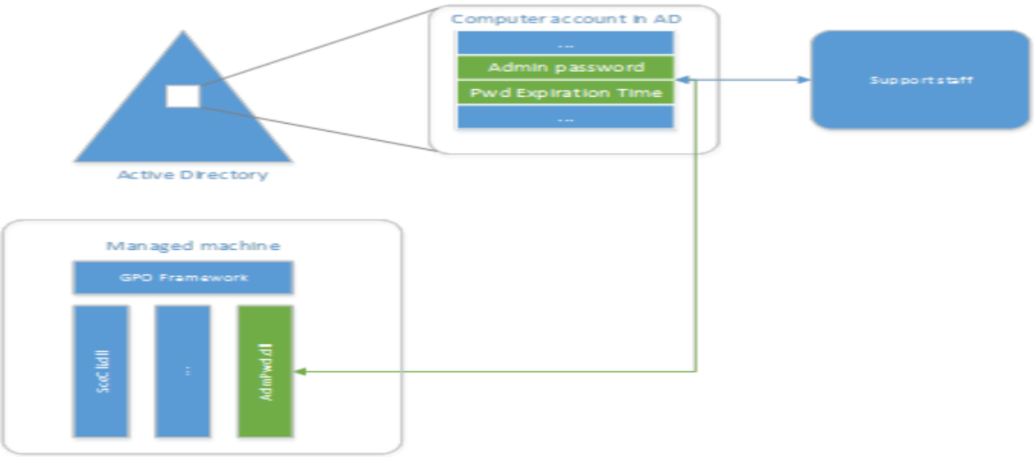
If you want to know more about LAPS – check out below link.

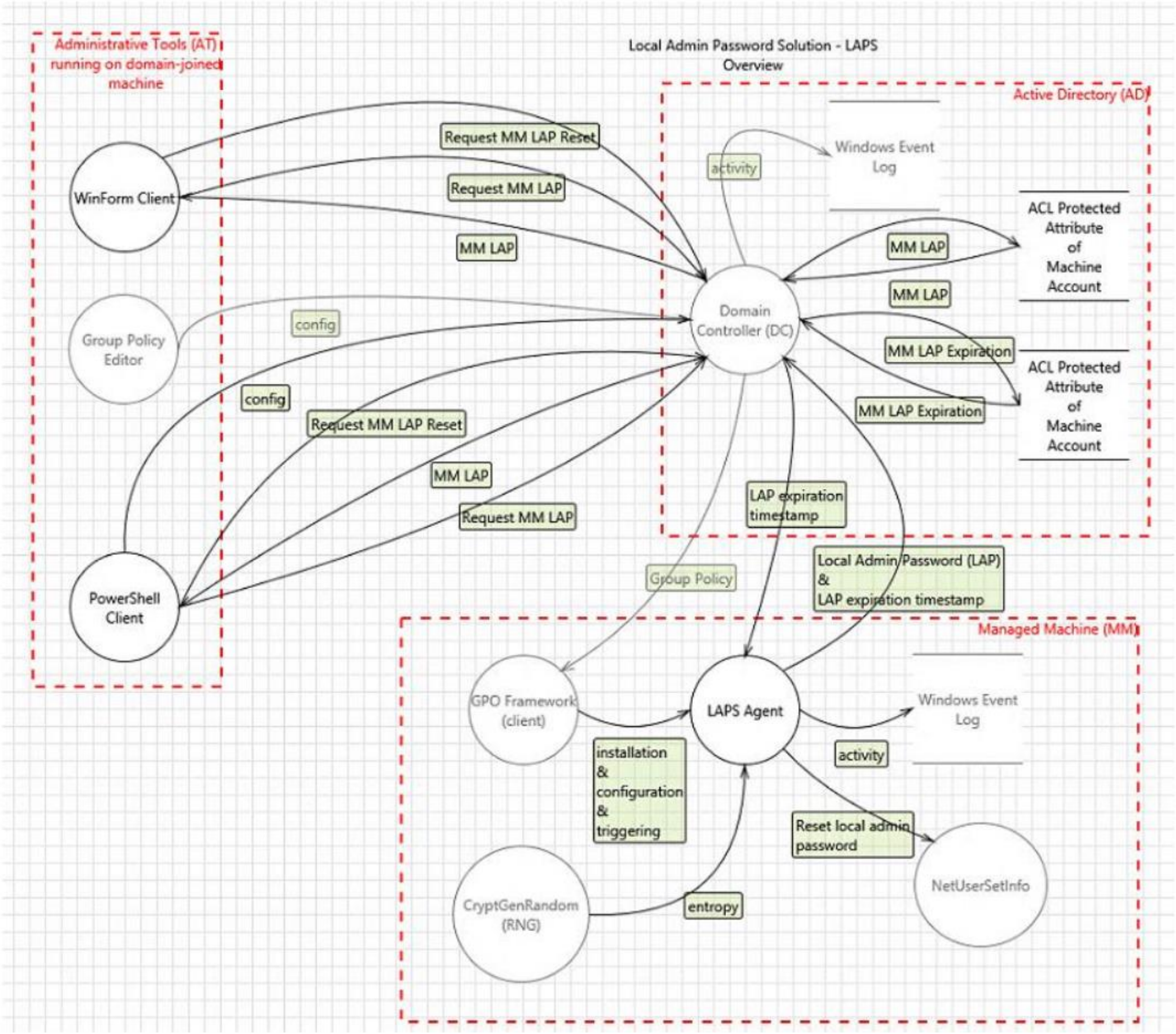
https://technet.microsoft.com/en-us/mt227395.aspx?f=255&MSPPError=-2147217396

Deployment Steps

1. Installs LAPS onto management machine
2. Extend Schema and prepare Active Directory
3. Configure Group Policy to enable and set the relevant policies
4. Deploying LAPS client to those machines you wish to manage

Here is the LAPS layout

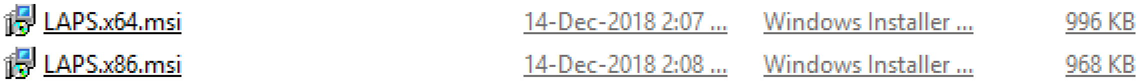




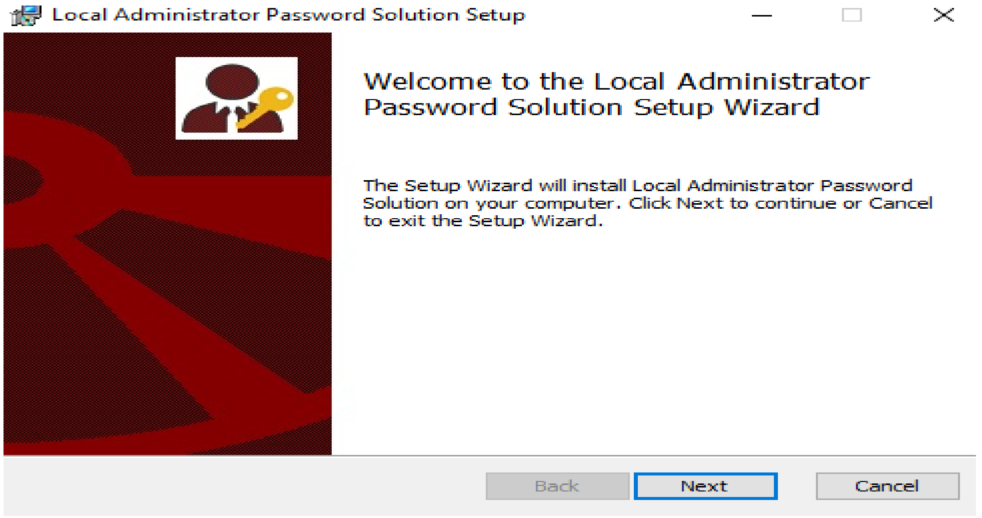
PRE-REQUISITE

Download both x86 and x64 version as this MSI will be deployed on clients to be managed
Detailed documentation is also available from that link
Active Directory requirement
Windows Server 2003 SP1 and above
Minimum OS requirement
Vista with current SP and above
Windows Server 2003 with current SP and above
.NET Framework 4.0
PowerShell 2.0 and above

1. Installing LAPS onto a machine (in my case Domain Controller):



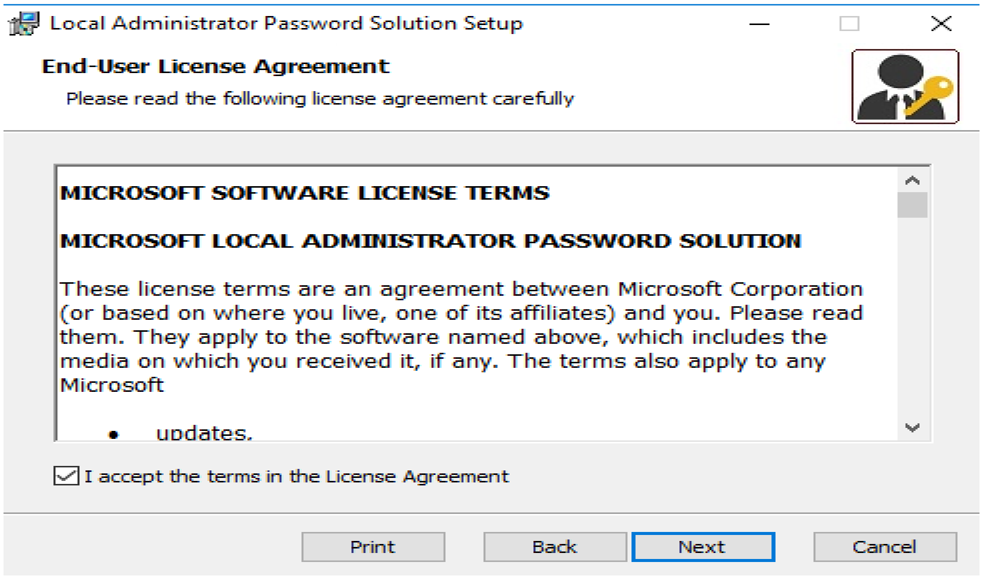
LAPS.x64.msi	14-Dec-2018 2:07 ...	Windows Installer ...	996 KB
LAPS.x86.msi	14-Dec-2018 2:08 ...	Windows Installer ...	968 KB



Local Administrator Password Solution Setup

Welcome to the Local Administrator Password Solution Setup Wizard

The Setup Wizard will install Local Administrator Password Solution on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



Local Administrator Password Solution Setup

End-User License Agreement

Please read the following license agreement carefully

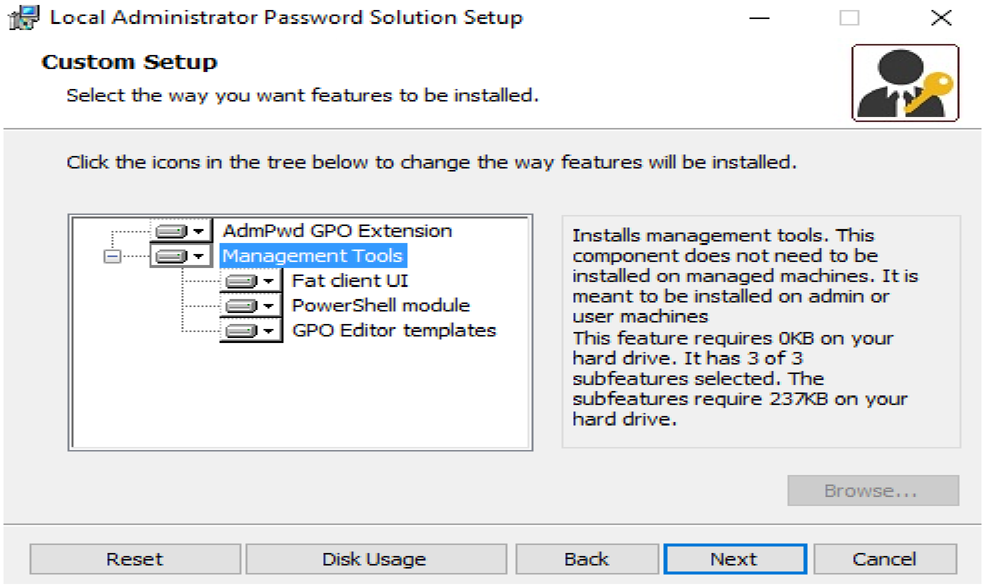
MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT LOCAL ADMINISTRATOR PASSWORD SOLUTION

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,

☑ I accept the terms in the License Agreement



Local Administrator Password Solution Setup

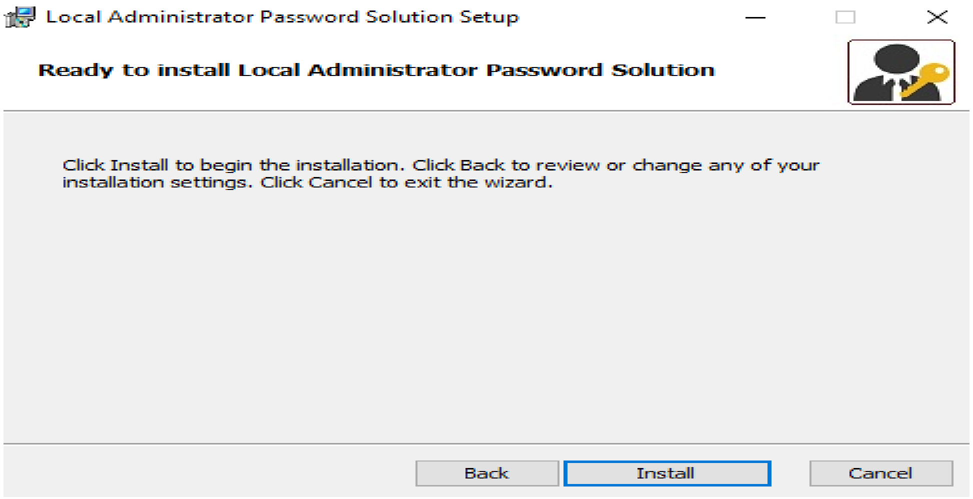
Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- AdmPwd GPO Extension
- Management Tools
  - Fat client UI
  - PowerShell module
  - GPO Editor templates

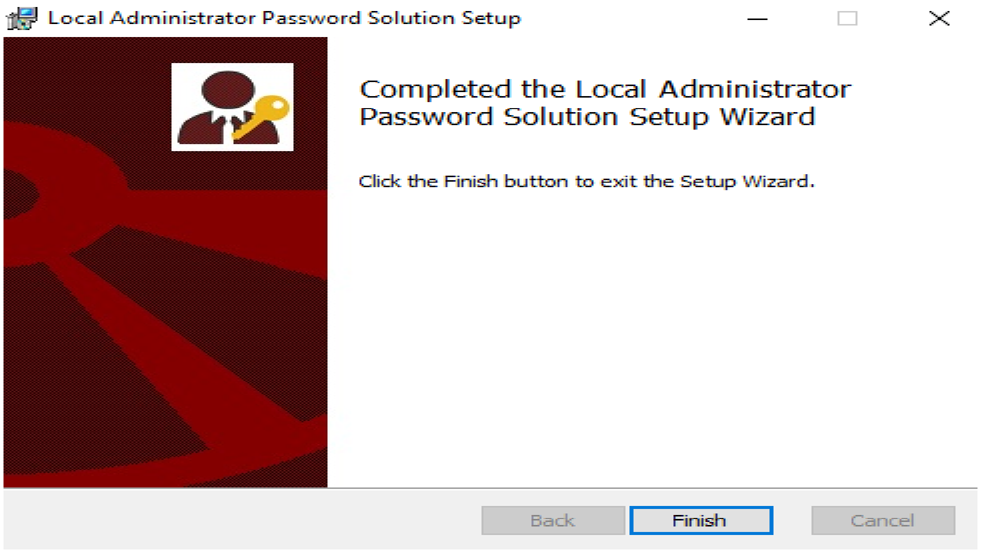
Installs management tools. This component does not need to be installed on managed machines. It is meant to be installed on admin or user machines
This feature requires 0KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 237KB on your hard drive.



Local Administrator Password Solution Setup

Ready to install Local Administrator Password Solution

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.



Local Administrator Password Solution Setup

Completed the Local Administrator Password Solution Setup Wizard

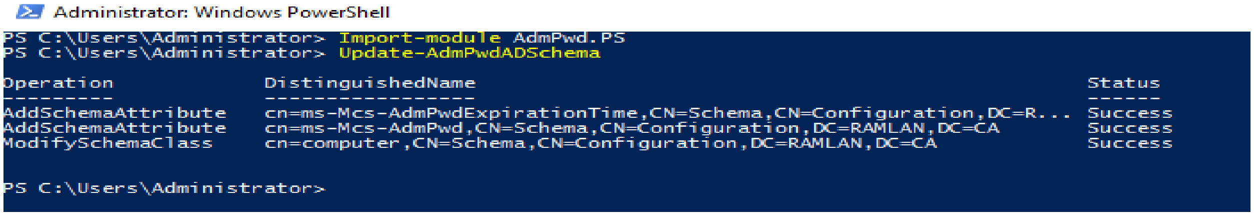
Click the Finish button to exit the Setup Wizard.

2. How to configure Active directory for LAPS

To update the Schema, you first need to import the PowerShell module. Open up an Administrative PowerShell window and use the below command:

Import-module AdmPwd.PS
Update-AdmPwdADSchema (This command updates the schema)

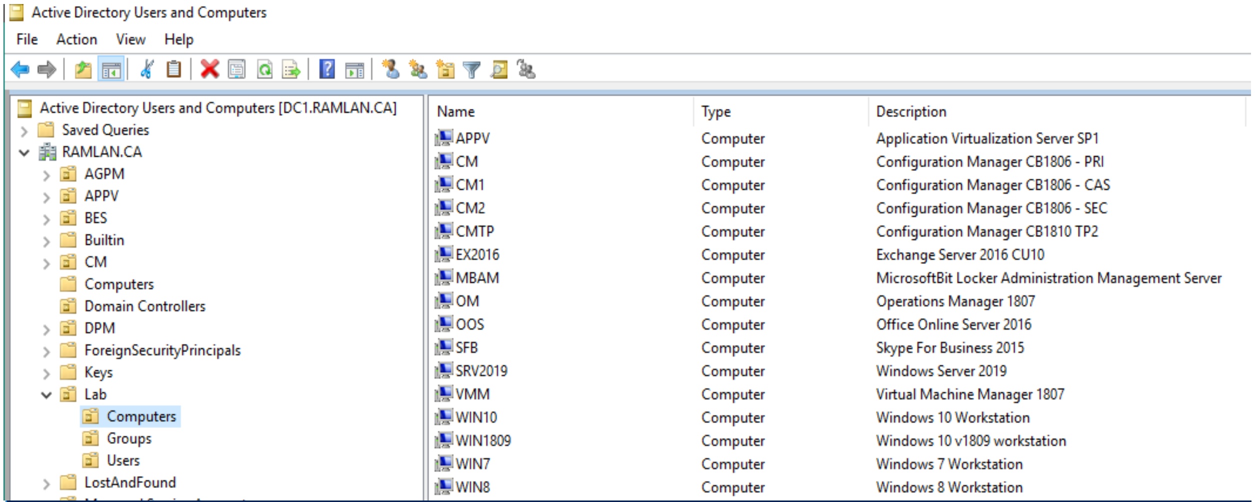
Once you run the above commands, you will find the status of operation as Success.



```
PS C:\Users\Administrator> Import-module AdmPwd.PS
PS C:\Users\Administrator> Update-AdmPwdADSchema

Operation             DistinguishedName                                              Status
---------             -----------------                                              ------
AddSchemaAttribute    cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=R... Success
AddSchemaAttribute    cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=RAMLAN,DC=CA       Success
ModifySchemaClass     cn=computer,CN=Schema,CN=Configuration,DC=RAMLAN,DC=CA           Success


PS C:\Users\Administrator>
```

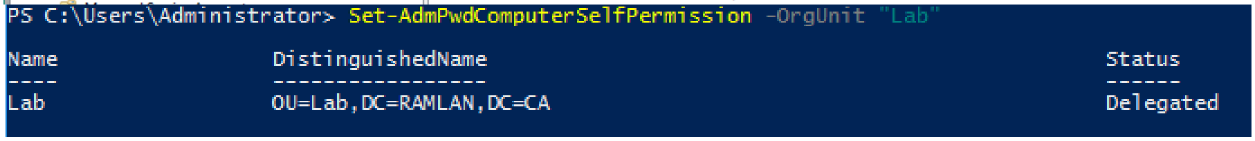
Next, we need to grant computers the ability to update their password attribute. The command is Set-AdmPwdComputerSelfPermission -OrgUnit

In my lab the computers are at **Lab** OU. I am going to grant computers in this OU the ability to update their password.



Active Directory Users and Computers [DC1.RAMLAN.CA]
- Saved Queries
- RAMLAN.CA
  - AGPM
  - APPV
  - BES
  - Builtin
  - CM
  - Computers
  - Domain Controllers
  - DPM
  - ForeignSecurityPrincipals
  - Keys
  - Lab
    - Computers
    - Groups
    - Users
  - LostAndFound

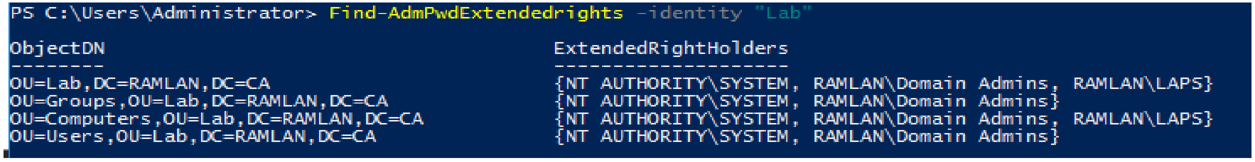
Name	Type	Description
APPV	Computer	Application Virtualization Server SP1
CM	Computer	Configuration Manager CB1806 - PRI
CM1	Computer	Configuration Manager CB1806 - CAS
CM2	Computer	Configuration Manager CB1806 - SEC
CMTP	Computer	Configuration Manager CB1810 TP2
EX2016	Computer	Exchange Server 2016 CU10
MBAM	Computer	MicrosoftBit Locker Administration Management Server
OM	Computer	Operations Manager 1807
OOS	Computer	Office Online Server 2016
SFB	Computer	Skype For Business 2015
SRV2019	Computer	Windows Server 2019
VMM	Computer	Virtual Machine Manager 1807
WIN10	Computer	Windows 10 Workstation
WIN1809	Computer	Windows 10 v1809 workstation
WIN7	Computer	Windows 7 Workstation
WIN8	Computer	Windows 8 Workstation



```
PS C:\Users\Administrator> Set-AdmPwdComputerSelfPermission -OrgUnit "Lab"

Name                DistinguishedName                                 Status
----                -----------------                                 ------
Lab                 OU=Lab,DC=RAMLAN,DC=CA                            Delegated
```

To quickly find which security principals have extended rights to the OU you can use PowerShell cmdlet.

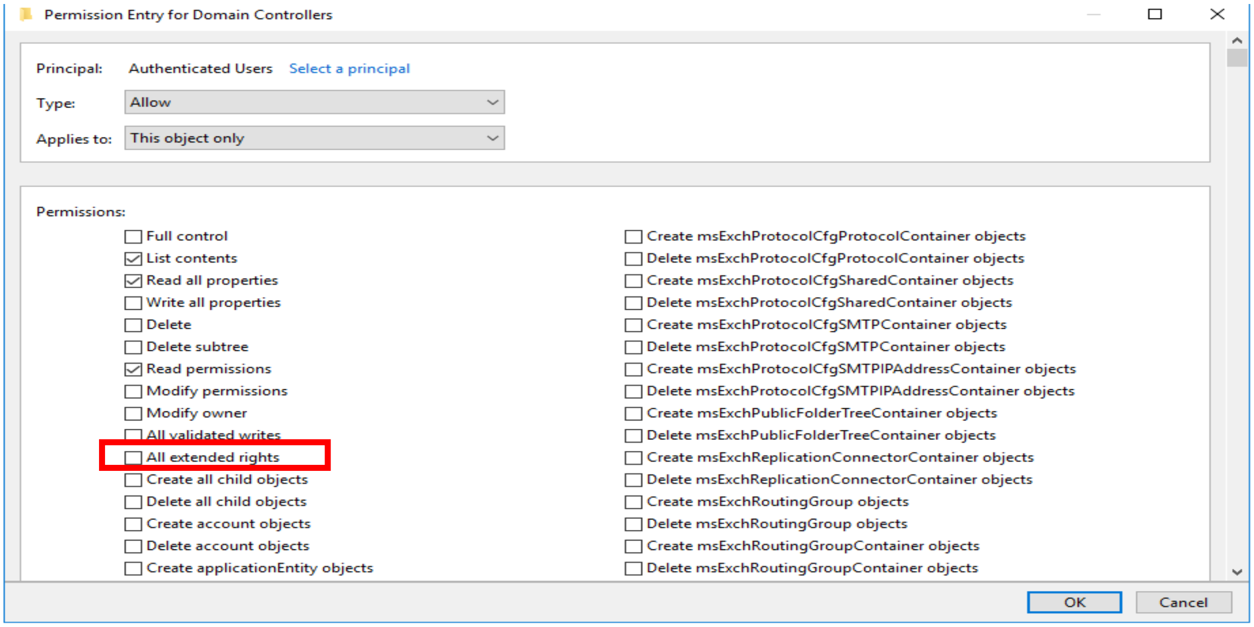
Find-AdmPwdExtendedrights -identity “Lab”



```
PS C:\Users\Administrator> Find-AdmPwdExtendedrights -identity "Lab"

ObjectDN                                      ExtendedRightHolders
--------                                      --------------------
OU=Lab,DC=RAMLAN,DC=CA                        {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins, RAMLAN\LAPS}
OU=Groups,OU=Lab,DC=RAMLAN,DC=CA              {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins}
OU=Computers,OU=Lab,DC=RAMLAN,DC=CA           {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins, RAMLAN\LAPS}
OU=Users,OU=Lab,DC=RAMLAN,DC=CA               {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins}
```

Removing the extended rights – For this, I choose Authenticated Users as an example

1. Open ADSIEdit
2. Right Click on the OU that contains the computer accounts that you are installing this solution on and select Properties
3. Click the Security tab
4. Click Advanced
5. Select the Group(s) or User(s) that you don't want to be able to read the password and then click Edit
6. Uncheck All extended rights



Permission Entry for Domain Controllers

Principal: Authenticated Users Select a principal

Type: Allow

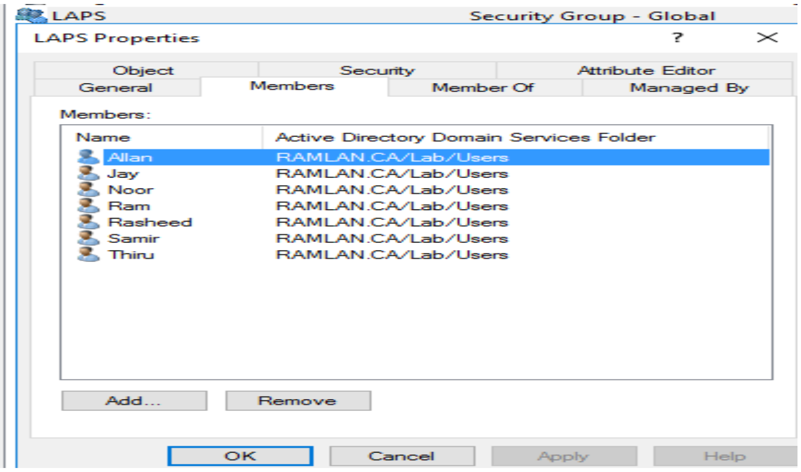
Applies to: This object only

Permissions:

- □ Full control
- ☑ List contents
- ☑ Read all properties
- □ Write all properties
- □ Delete
- □ Delete subtree
- ☑ Read permissions
- □ Modify permissions
- □ Modify owner
- □ All validated writes
- □ All extended rights
- □ Create all child objects
- □ Delete all child objects
- □ Create account objects
- □ Delete account objects
- □ Create applicationEntity objects
- □ Create msExchProtocolCfgProtocolContainer objects
- □ Delete msExchProtocolCfgProtocolContainer objects
- □ Create msExchProtocolCfgSharedContainer objects
- □ Delete msExchProtocolCfgSharedContainer objects
- □ Create msExchProtocolCfgSMTPContainer objects
- □ Delete msExchProtocolCfgSMTPContainer objects
- □ Create msExchProtocolCfgSMTPIPAddressContainer objects
- □ Delete msExchProtocolCfgSMTPIPAddressContainer objects
- □ Create msExchPublicFolderTreeContainer objects
- □ Delete msExchPublicFolderTreeContainer objects
- □ Create msExchReplicationConnectorContainer objects
- □ Delete msExchReplicationConnectorContainer objects
- □ Create msExchRoutingGroup objects
- □ Delete msExchRoutingGroup objects
- □ Create msExchRoutingGroupContainer objects
- □ Delete msExchRoutingGroupContainer objects

Delegate a Security group the rights to view and reset LAPS

For this, I created a security group called LAPS and added few Support users who are members of this group.



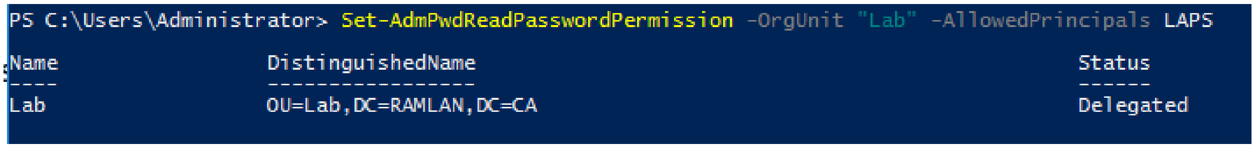
LAPS Security Group - Global

LAPS Properties

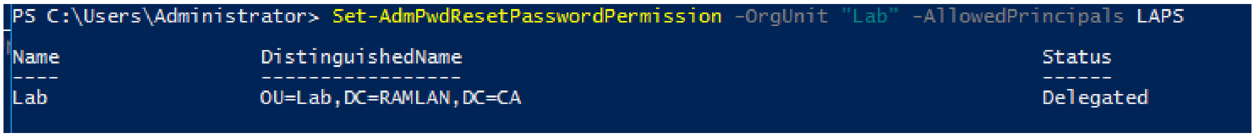
Members:

Name	Active Directory Domain Services Folder
Allan	RAMLAN.CA/Lab/Users
Jay	RAMLAN.CA/Lab/Users
Noor	RAMLAN.CA/Lab/Users
Ram	RAMLAN.CA/Lab/Users
Rasheed	RAMLAN.CA/Lab/Users
Samir	RAMLAN.CA/Lab/Users
Thiru	RAMLAN.CA/Lab/Users

With this command any computers in this OU & users/group has right to view and reset the password

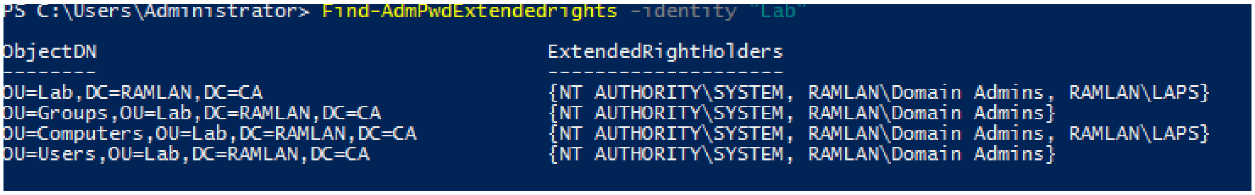


```
PS C:\Users\Administrator> Set-AdmPwdReadPasswordPermission -OrgUnit "Lab" -AllowedPrincipals LAPS

Name                DistinguishedName                                                  Status
----                -----------------                                                  ------
Lab                 OU=Lab,DC=RAMLAN,DC=CA                                             Delegated
```



```
PS C:\Users\Administrator> Set-AdmPwdResetPasswordPermission -OrgUnit "Lab" -AllowedPrincipals LAPS

Name                DistinguishedName                                               Status
----                -----------------                                               ------
Lab                 OU=Lab,DC=RAMLAN,DC=CA                                          Delegated
```

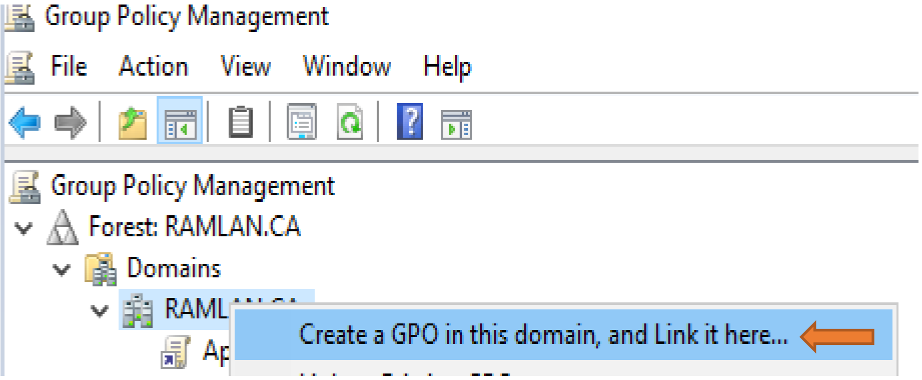
Below command will list who has rights to view and reset password for computers in this OU.

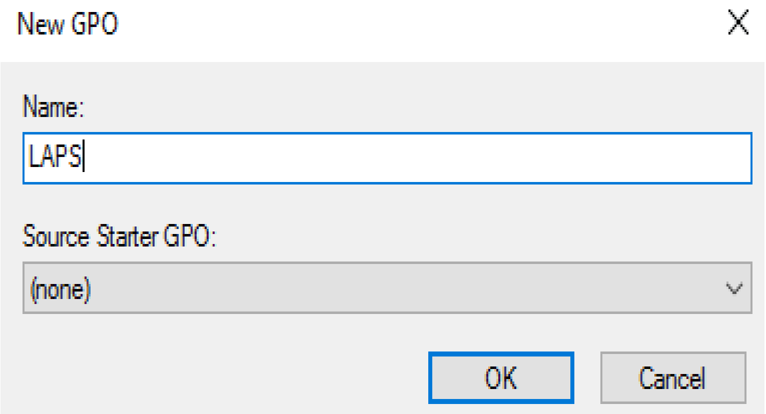


```
PS C:\Users\Administrator> Find-AdmPwdExtendedrights -identity "Lab"

ObjectDN                                      ExtendedRightHolders
--------                                      --------------------
OU=Lab,DC=RAMLAN,DC=CA                        {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins, RAMLAN\LAPS}
OU=Groups,OU=Lab,DC=RAMLAN,DC=CA              {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins}
OU=Computers,OU=Lab,DC=RAMLAN,DC=CA           {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins, RAMLAN\LAPS}
OU=Users,OU=Lab,DC=RAMLAN,DC=CA               {NT AUTHORITY\SYSTEM, RAMLAN\Domain Admins}
```

3. How to configure Group Policy for LAPS

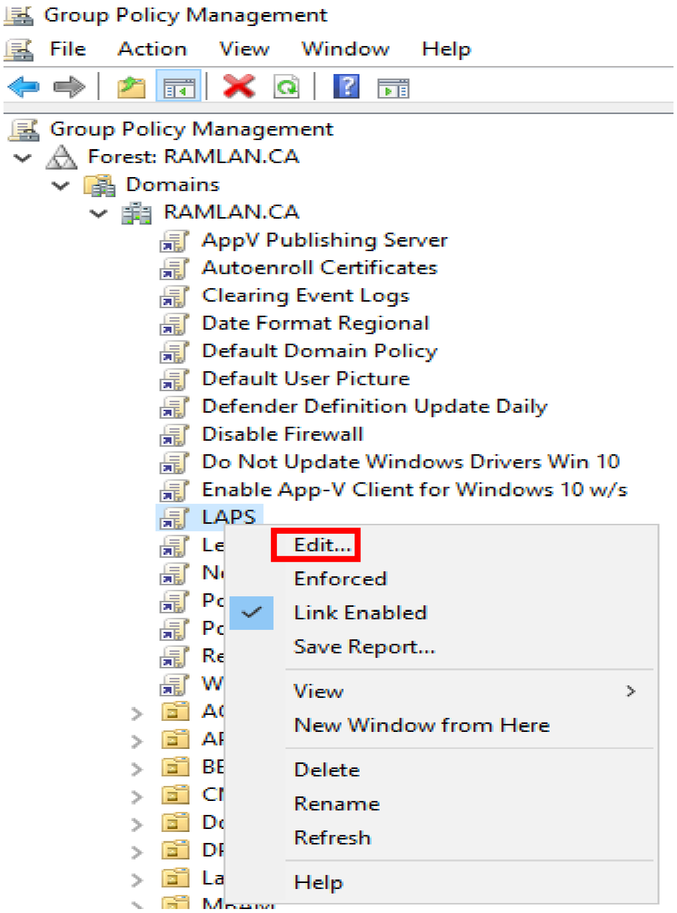
Launch GPMC



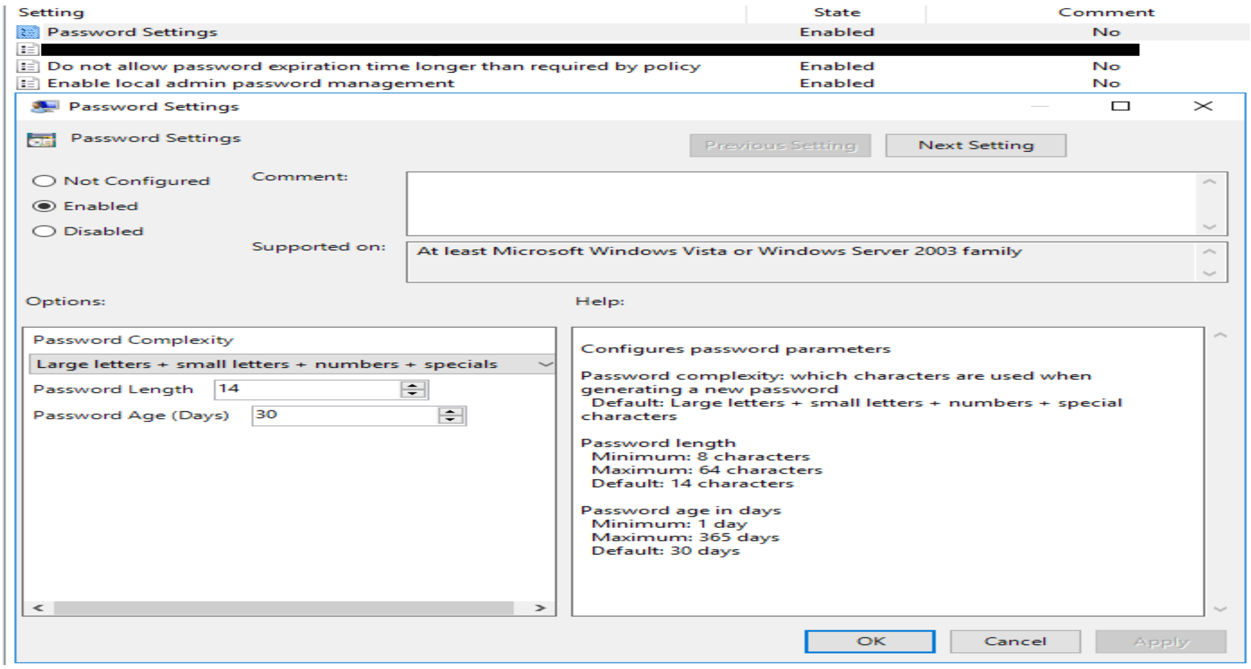


Name: LAPS

Source Starter GPO: (none)



The settings are located under Computer Configuration > Administrative Templates > LAPS



Setting	State	Comment
Password Settings	Enabled	No
[redacted]		
Do not allow password expiration time longer than required by policy	Enabled	No
Enable local admin password management	Enabled	No

Password Settings

Password Settings

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows Vista or Windows Server 2003 family

Options:

Password Complexity
Large letters + small letters + numbers + specials
Password Length 14
Password Age (Days) 30

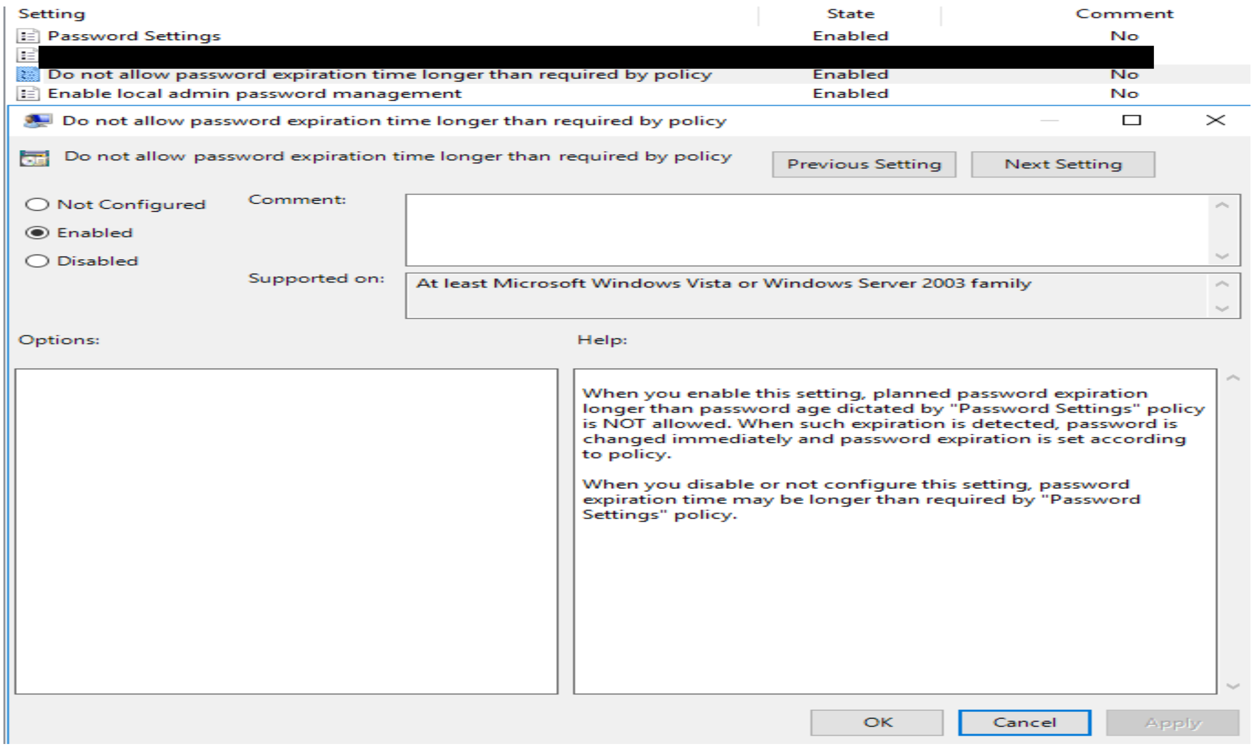
Help:

Configures password parameters

Password complexity: which characters are used when generating a new password
Default: Large letters + small letters + numbers + special characters

Password length
Minimum: 8 characters
Maximum: 64 characters
Default: 14 characters

Password age in days
Minimum: 1 day
Maximum: 365 days
Default: 30 days



Setting	State	Comment
Password Settings	Enabled	No
[redacted]	[redacted]	[redacted]
Do not allow password expiration time longer than required by policy	Enabled	No
Enable local admin password management	Enabled	No

Do not allow password expiration time longer than required by policy

Do not allow password expiration time longer than required by policy

○ Not Configured
● Enabled
○ Disabled

Comment:

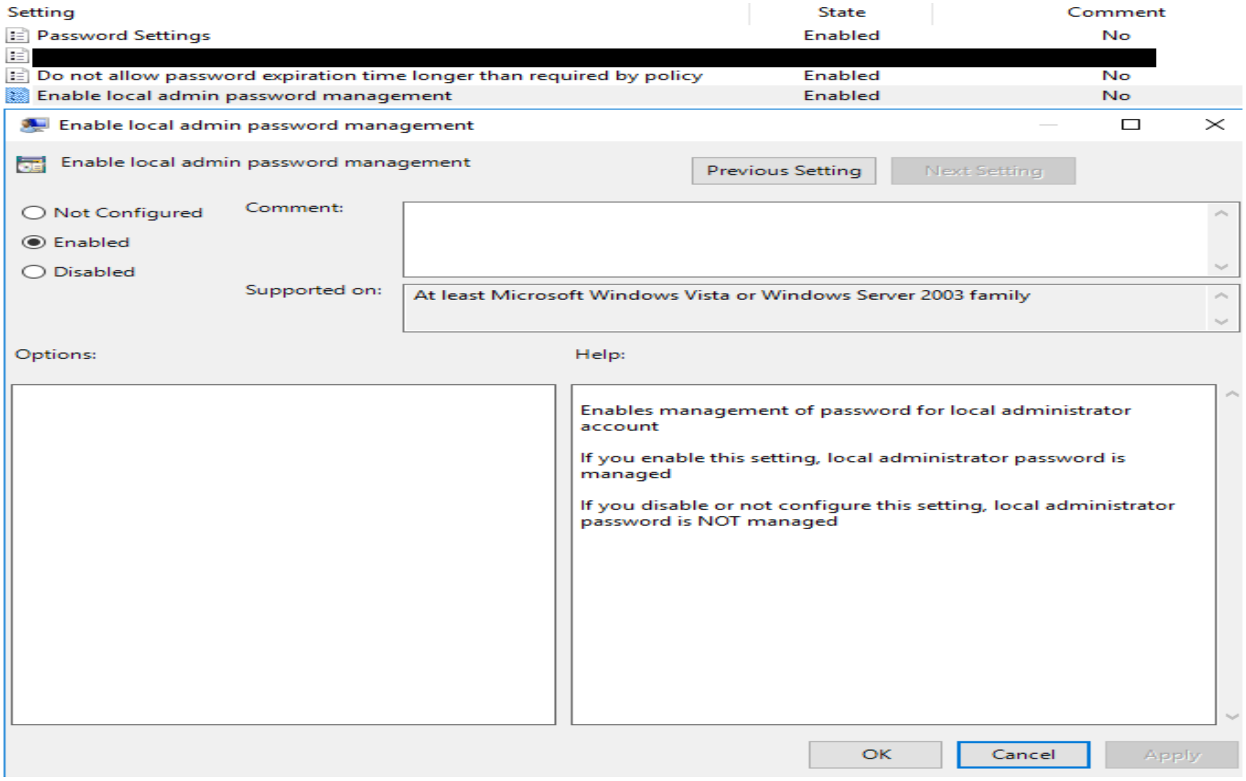
Supported on: At least Microsoft Windows Vista or Windows Server 2003 family

Options:

Help:

When you enable this setting, planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed. When such expiration is detected, password is changed immediately and password expiration is set according to policy.

When you disable or not configure this setting, password expiration time may be longer than required by "Password Settings" policy.



Setting	State	Comment
Password Settings	Enabled	No
[redacted]	[redacted]	[redacted]
Do not allow password expiration time longer than required by policy	Enabled	No
Enable local admin password management	Enabled	No

Enable local admin password management

Enable local admin password management

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows Vista or Windows Server 2003 family

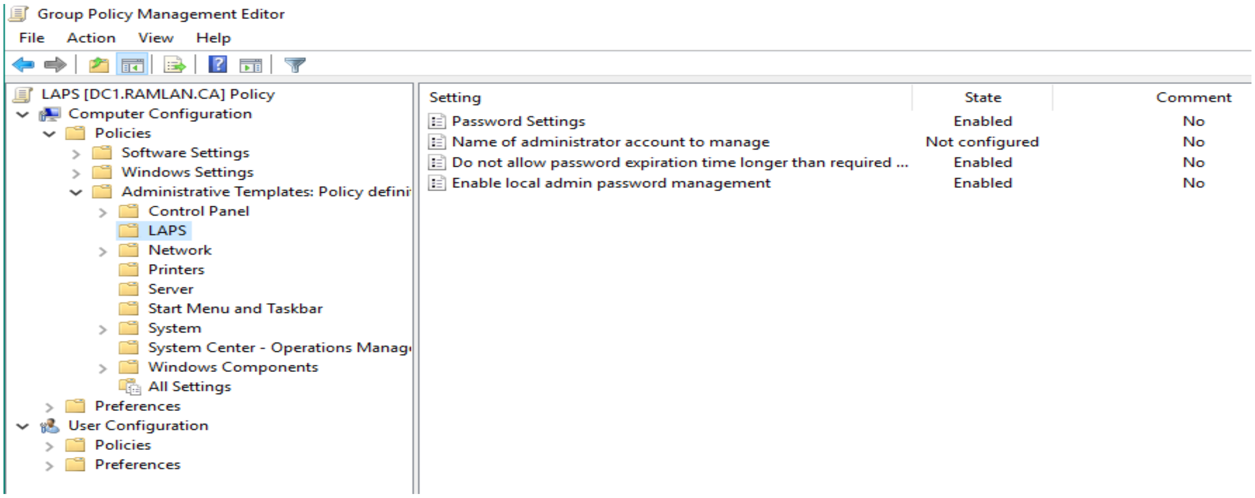
Options:

Help:

Enables management of password for local administrator account

If you enable this setting, local administrator password is managed

If you disable or not configure this setting, local administrator password is NOT managed

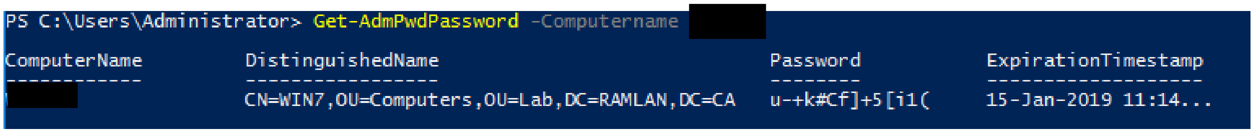


Setting	State	Comment
Password Settings	Enabled	No
Name of administrator account to manage	Not configured	No
Do not allow password expiration time longer than required ...	Enabled	No
Enable local admin password management	Enabled	No

4. CLIENTS TO BE MANAGED

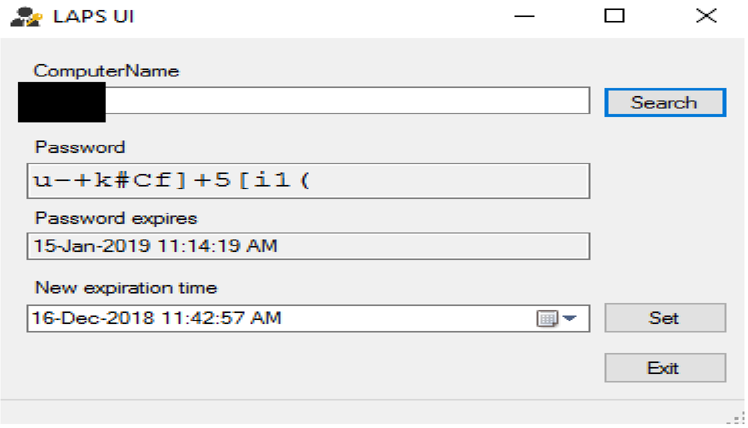
To manage a client, we must install LAPS on it by using the same MSI files downloaded in the prerequisite section.

We can create a package within SCCM or deploy MSI manually. For the purpose of testing, I have installed manually. Now it is time to test the implementation. I will run below command to find out the password and expiration time



```
PS C:\Users\Administrator> Get-AdmPwdPassword -Computername [redacted]

ComputerName        DistinguishedName                      Password        ExpirationTimestamp
------------        -----------------                      --------        -------------------
[redacted]          CN=WIN7,OU=Computers,OU=Lab,DC=RAMLAN,DC=CA   u-+k#Cf]+5[i1(    15-Jan-2019 11:14...
```

It is working. We can also use Laps UI (Start – Programs – Laps – LAPS UI) from Domain Controller to find out the password



ComputerName: [redacted]

Password: u-+k#Cf]+5[i1(

Password expires: 15-Jan-2019 11:14:19 AM

New expiration time: 16-Dec-2018 11:42:57 AM

This completes the whole process of deploying LAPS on Windows Server 2016.

Thanks

Ram Lan
16th Dec 2018

COMMANDS USED FOR THIS DEPLOYMENT:

```
Import-module AdmPwd.PS
Update-AdmPwdADSchema
Set-AdmPwdComputerSelfPermission -OrgUnit "Lab"
Set-AdmPwdReadPasswordPermission -OrgUnit "Lab" -AllowedPrincipals LAPS
Set-AdmPwdResetPasswordPermission -OrgUnit "Lab" -AllowedPrincipals LAPS
Find-AdmPwdExtendedrights -identity "Lab"
Get-AdmPwdPassword -Computername "XXXX"
msiexec /i LAPS.x64.msi /quiet
```