# Step by Step Guide to Deploy Microsoft LAPS

In this document I will show you step by step method to deploy Microsoft LAPS. The Local Administrator Password Solution (LAPS) provides management of local account passwords of domain joined computers. When LAPS is implemented, passwords are stored in Active Directory (AD) and protected by ACL, so only eligible users can read it or request its reset. For environments in which users are required to log on to computers without domain credentials, password management can become a complex issue. The Local Administrator Password Solution (LAPS) provides a solution to this issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain. Domain administrators using the solution can determine which users, such as helpdesk administrators, are authorized to read passwords.

Imagine a scenario where you have got lot of servers and workstations. When it is not possible to use domain account to log on to server and perform administrative tasks, you are in a big trouble.

Some scenarios that one could imagine without LAPS –

a) Machine loses connection to corporate network and there is not cached credential with administrative privileges.

b) Machine loses connection with domain or is accidentally dis-joined from domain, so domain credentials cannot be used to log on to the server and repair it.

For this type of support scenarios, support staff needs to know the password of local Administrator account to be able to log on to computer and perform necessary administrative tasks.

## What do I need before i deploy Microsoft LAPS ?.

To install Microsoft LAPS, you’ll need at least one management computer, and at least one client computer. In my case I am installing the Microsoft LAPS on my domain controller. There are some client machines that are part of domain, we will be deploying the LAPS software to these client machines as well.

### Supported Operating System

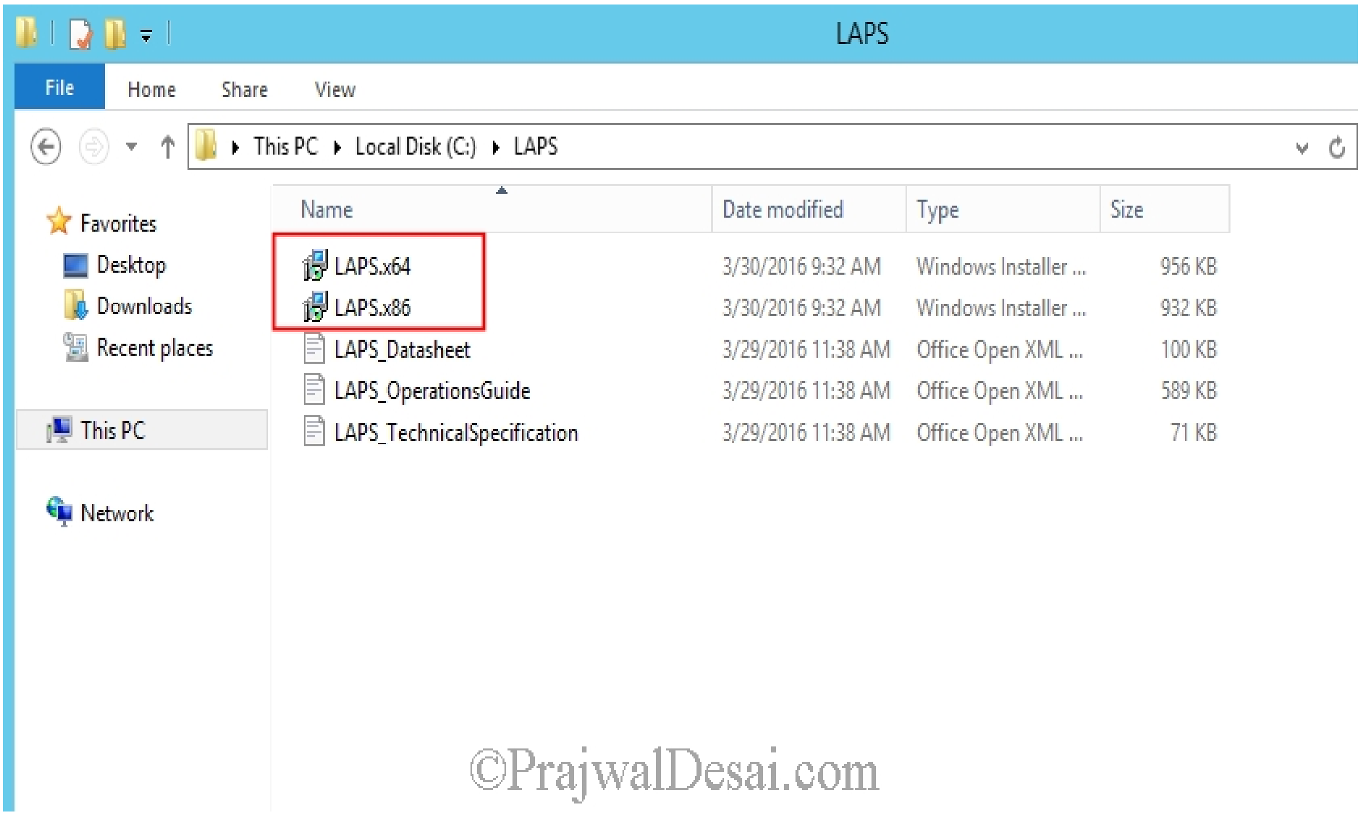
Windows 10 , Windows 7, Windows 8, Windows 8.1, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista
Active Directory: (requires AD schema extension) Windows 2003 SP1 or later.
Managed machines: Windows Server 2003 SP2 or later, or Windows Server 2003 x64 Edition SP2 or later.
Note: Itanium-based machines are not supported.
Management tools: .NET Framework 4.0 & PowerShell 2.0 or later

## How to install and deploy Microsoft LAPS Software

We’ll now install the LAPS fat client, PowerShell module and Group Policy templates on the management computer. Click on the below button to download the Microsoft LAPS software. You can download both 64 bit and 32 bit versions.

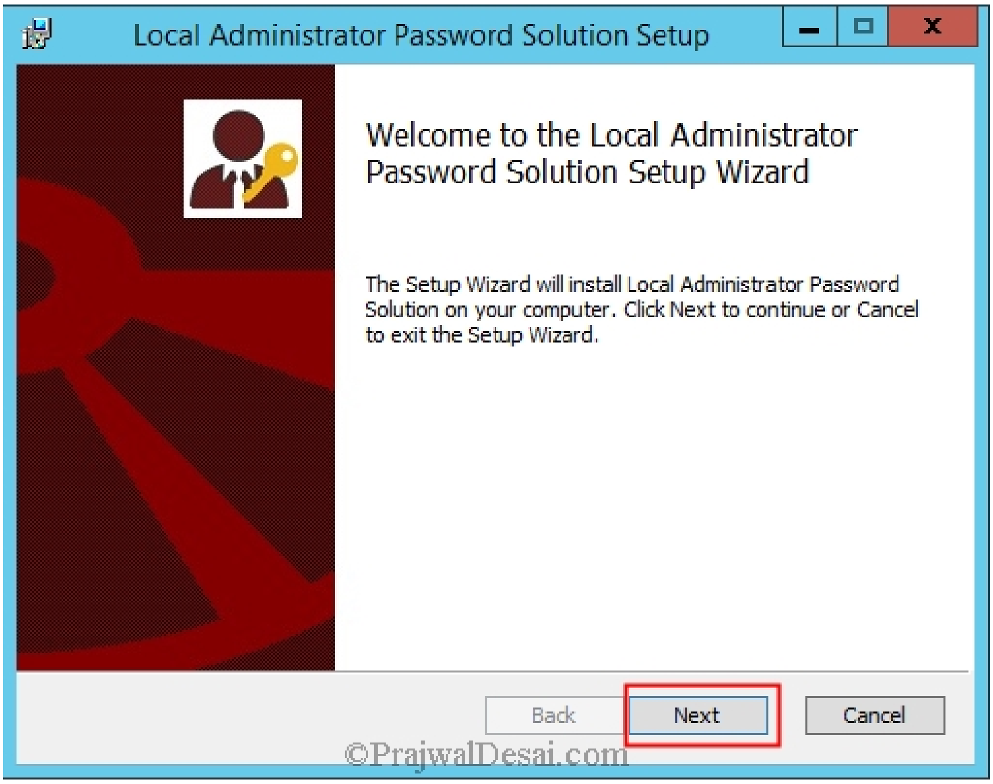
Download Microsoft Local Administrator Password Solution Software

Once you download the LAPS software, copy the msi files to a shared folder on the server. In my case I have created a shared folder on C drive and all the files downloaded are present there. Right click on LAPS x64 and click **install**.



| Name | Date modified | Type | Size |
|---|---|---|---|
| LAPS.x64 | 3/30/2016 9:32 AM | Windows Installer ... | 956 KB |
| LAPS.x86 | 3/30/2016 9:32 AM | Windows Installer ... | 932 KB |
| LAPS_Datasheet | 3/29/2016 11:38 AM | Office Open XML ... | 100 KB |
| LAPS_OperationsGuide | 3/29/2016 11:38 AM | Office Open XML ... | 589 KB |
| LAPS_TechnicalSpecification | 3/29/2016 11:38 AM | Office Open XML ... | 71 KB |

On the LAPS setup wizard, click **Next**.

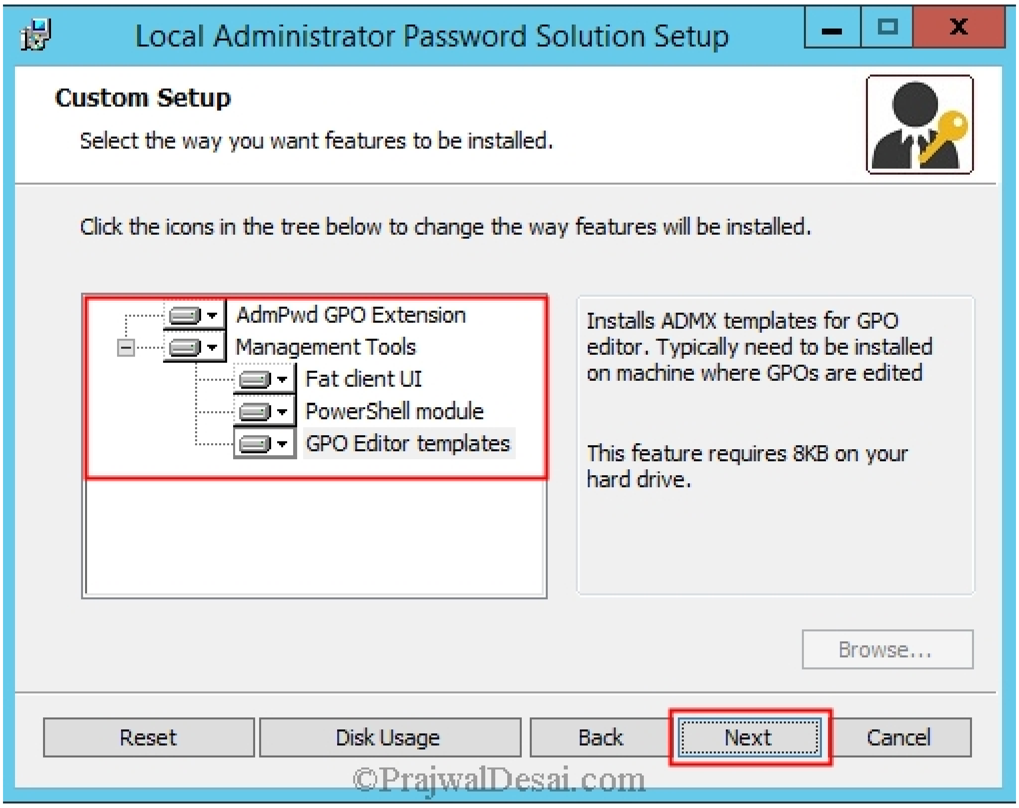


Local Administrator Password Solution Setup

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.

We will select all the features to be installed. Click **Next**.



Local Administrator Password Solution Setup

**Custom Setup**

Select the way you want features to be installed.

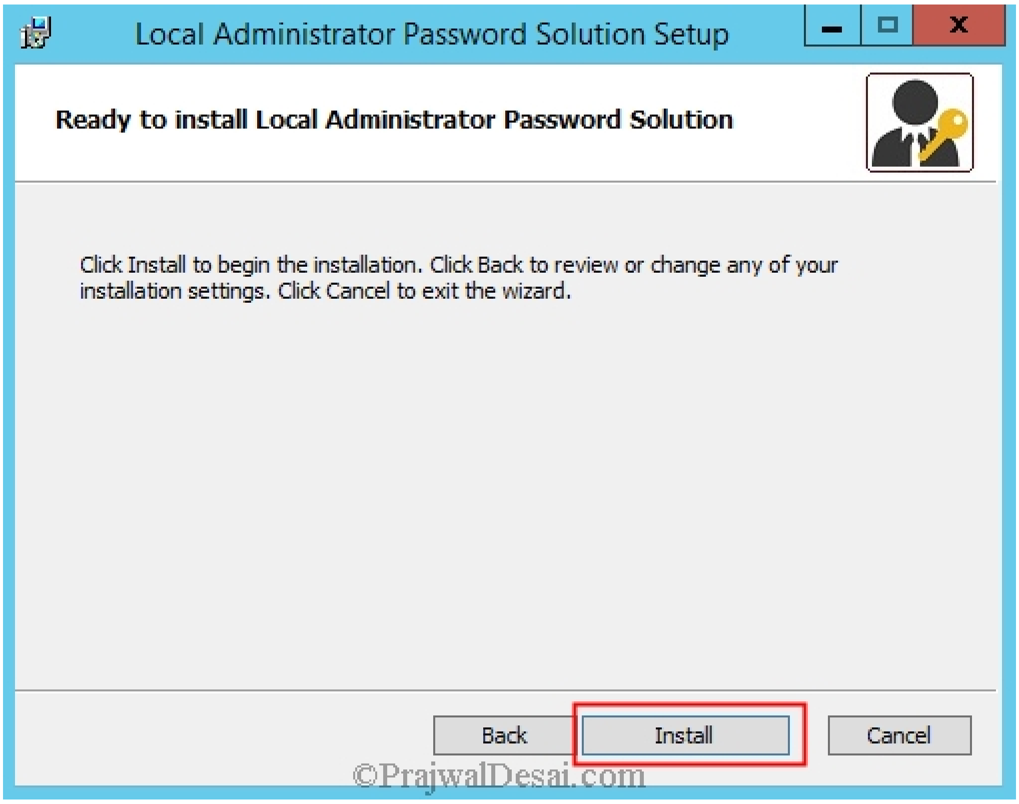
Click the icons in the tree below to change the way features will be installed.

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

Installs ADMX templates for GPO editor. Typically need to be installed on machine where GPOs are edited

This feature requires 8KB on your hard drive.

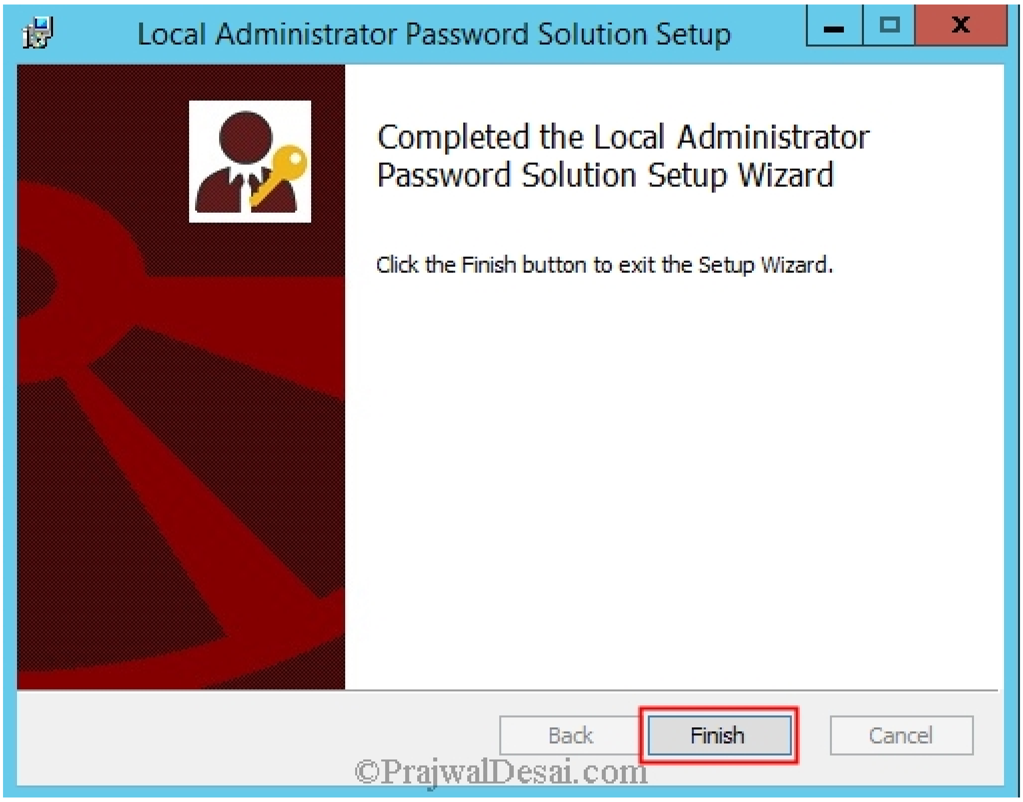
Click on **Install**.



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.

Click on **Finish**. The LAPS software has now been installed.



Completed the Local Administrator Password Solution Setup Wizard

Click the Finish button to exit the Setup Wizard.

## Deploying LAPS to the client machines using GPO

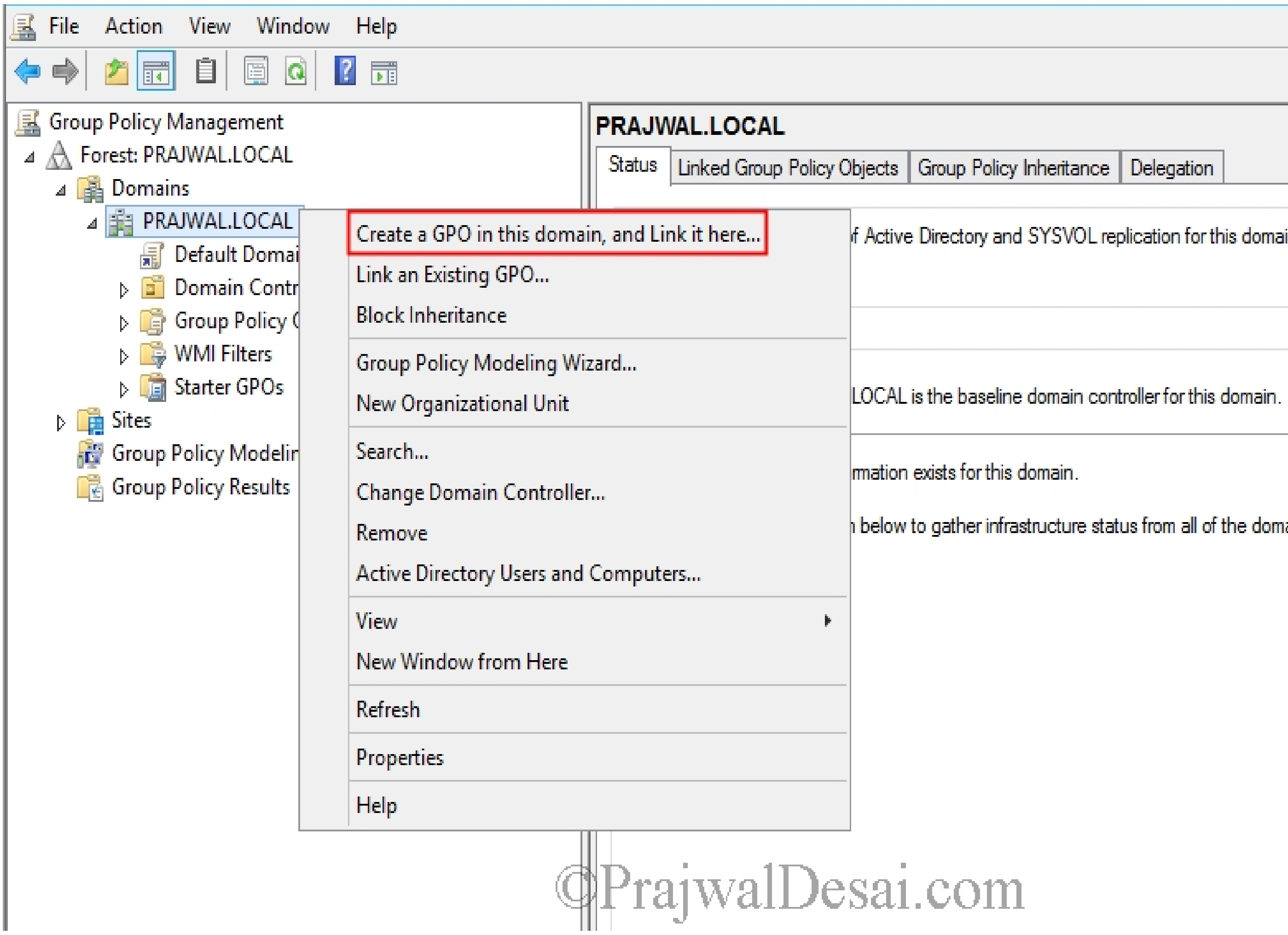
We will now configure a GPO to deploy the LAPS software to the client computer. You could also use scripting method to deploy LAPS. If you want to script this you can use this command line to do a silent install:

msiexec /i <file location>LAPS.x64.msi /quiet **or** msiexec /i <file location>LAPS.x86.msi /quiet

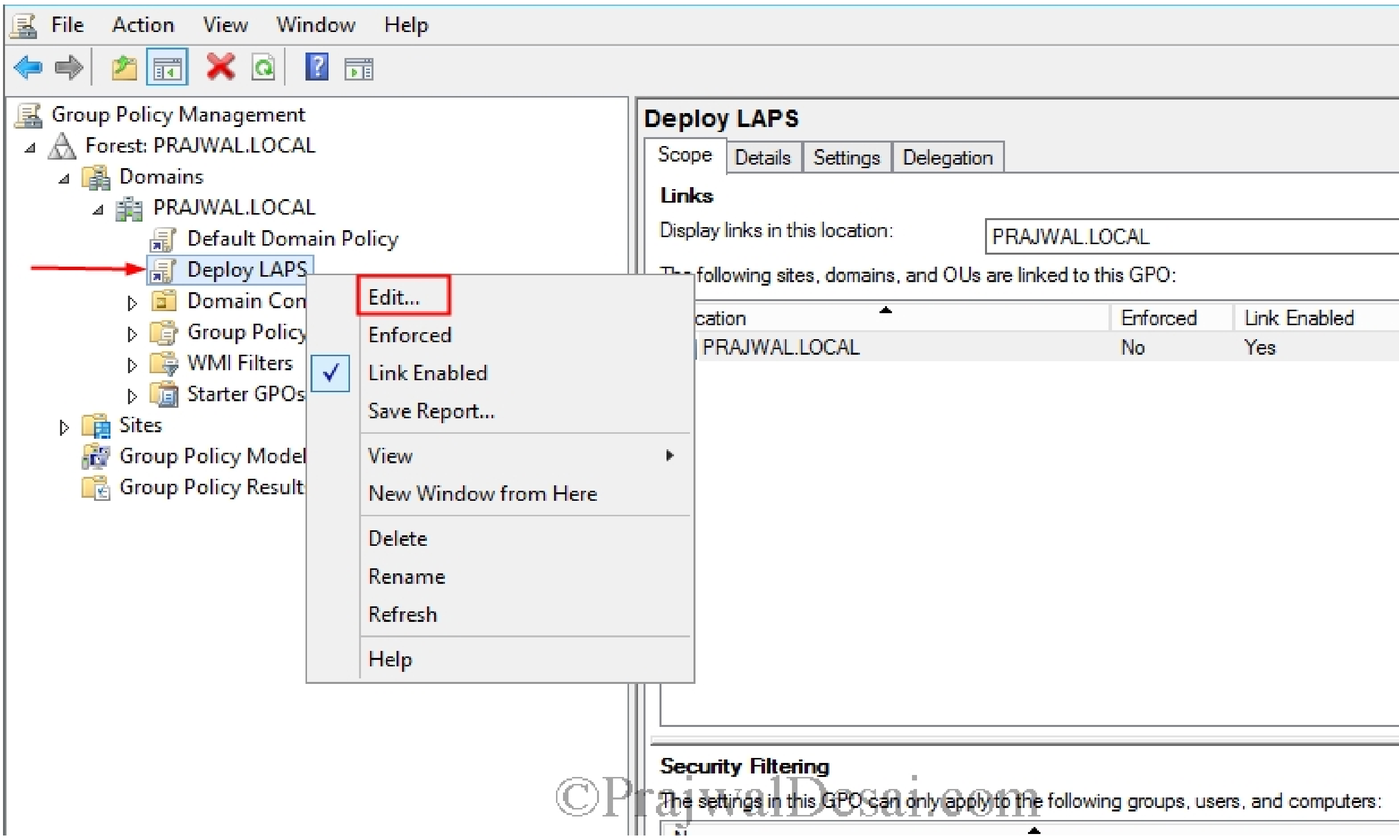
Just change the **<file location>** to a local or network path.

Alternative method of installation to managed clients is to copy the **AdmPwd.dll** to the target computer and use this command: **regsvr32.exe AdmPwd.dll**

Launch the Group Policy Management console, right click on the domain and click **Create a GPO in this domain and link it here**. Provide a name to the GPO.



Right click on the GPO and click **Edit**.



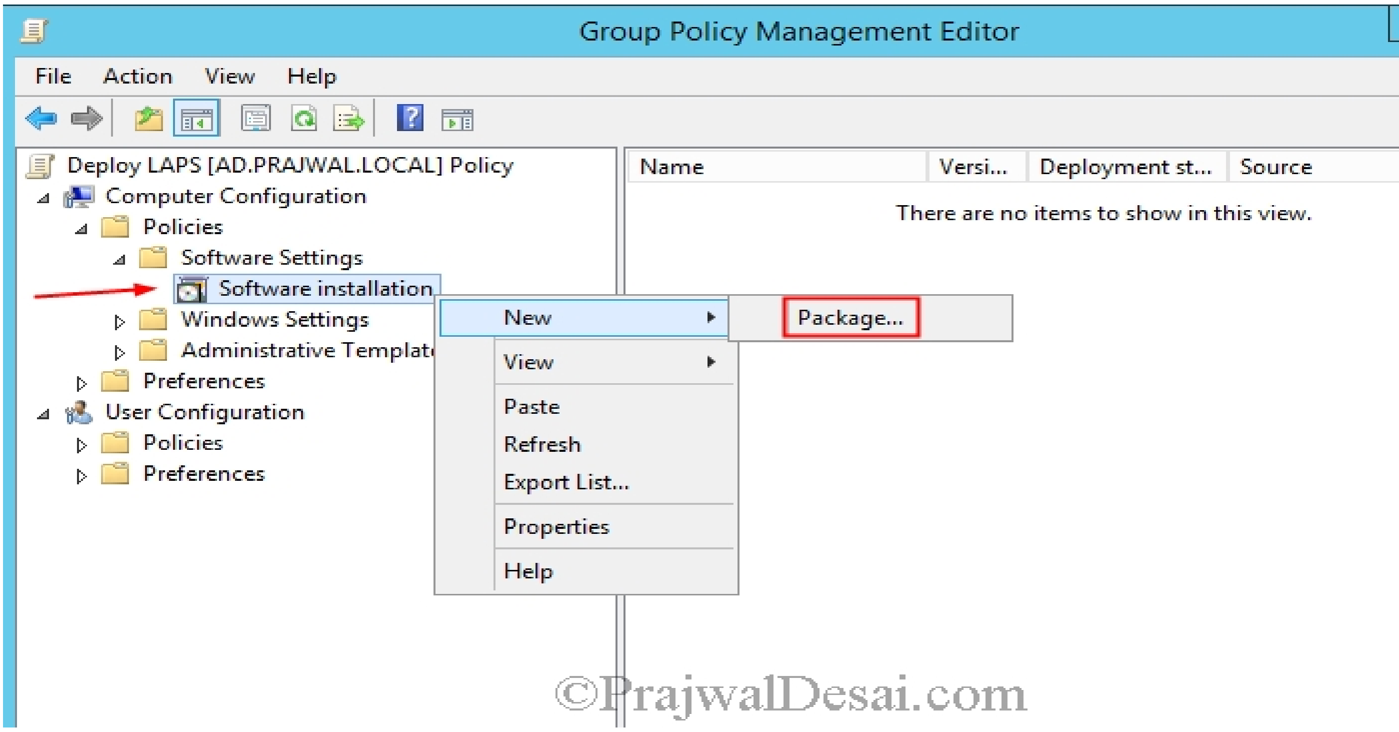
Display links in this location: PRAJWAL.LOCAL

The following sites, domains, and OUs are linked to this GPO:

| ...cation | Enforced | Link Enabled |
|---|---|---|
| PRAJWAL.LOCAL | No | Yes |

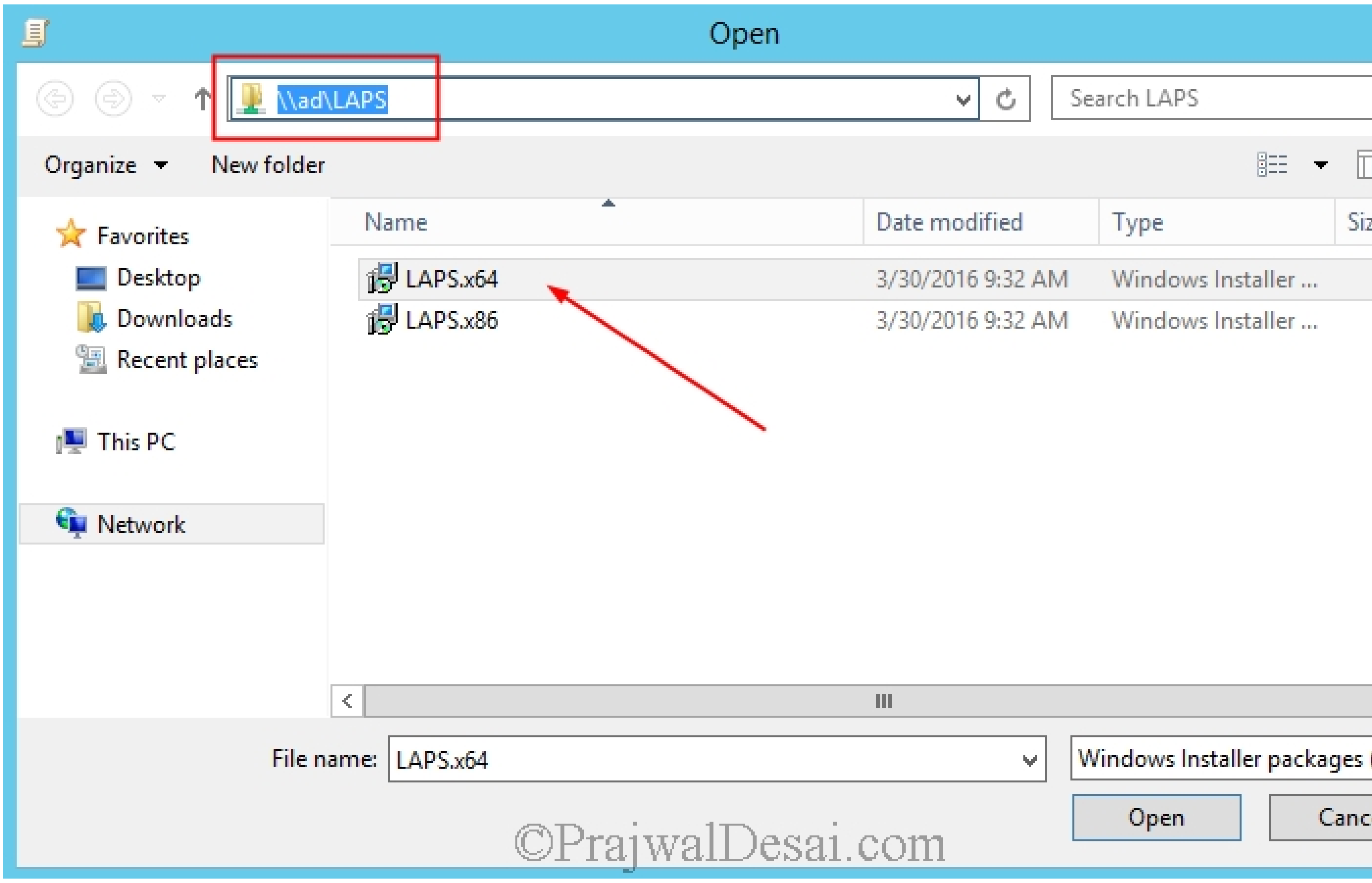
The settings in this GPO can only apply to the following groups, users, and computers:

In the GPM editor, expand Computer Configuration > Policies > Software Settings. Right click on **Software Installation** and click **New** > **Package**.



There are no items to show in this view.

Browse for the path where the files are located, select the LAPS software. Choose the **deployment method** as **Assigned** and click OK.

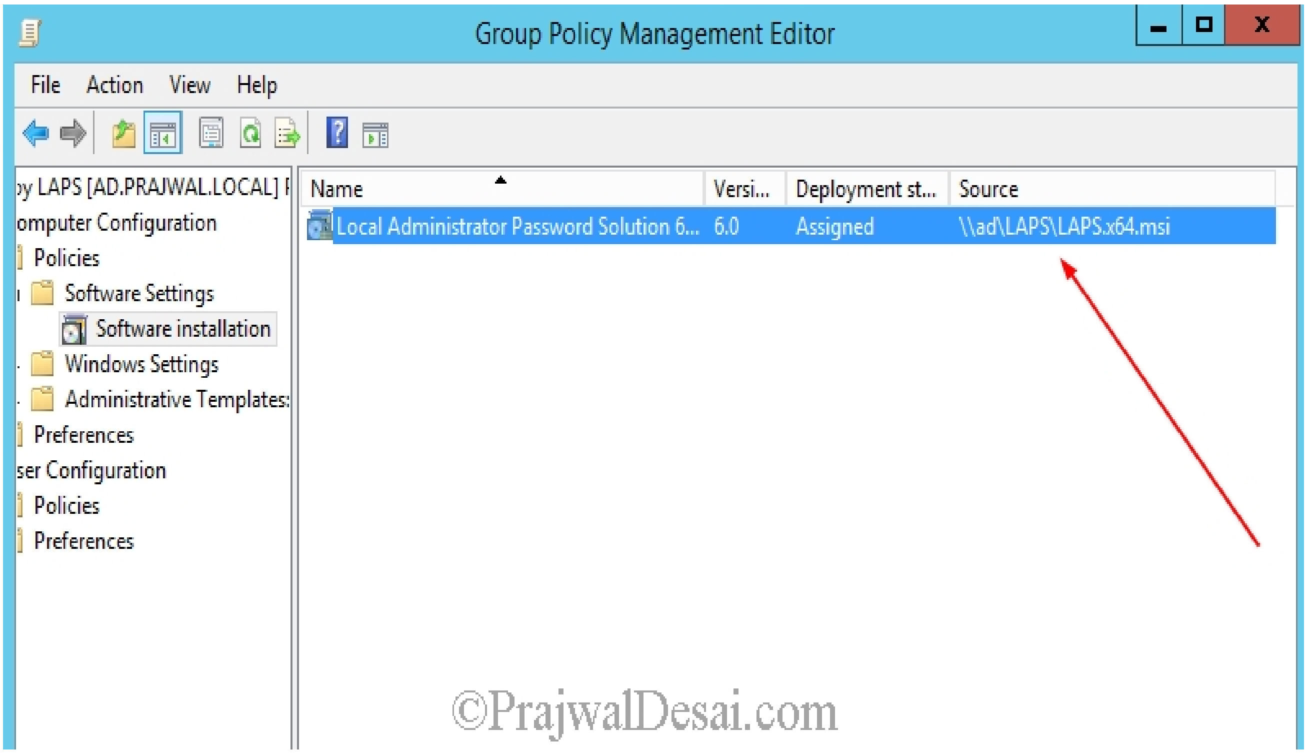


| Name | Date modified | Type |
|---|---|---|
| LAPS.x64 | 3/30/2016 9:32 AM | Windows Installer ... |
| LAPS.x86 | 3/30/2016 9:32 AM | Windows Installer ... |

File name: LAPS.x64

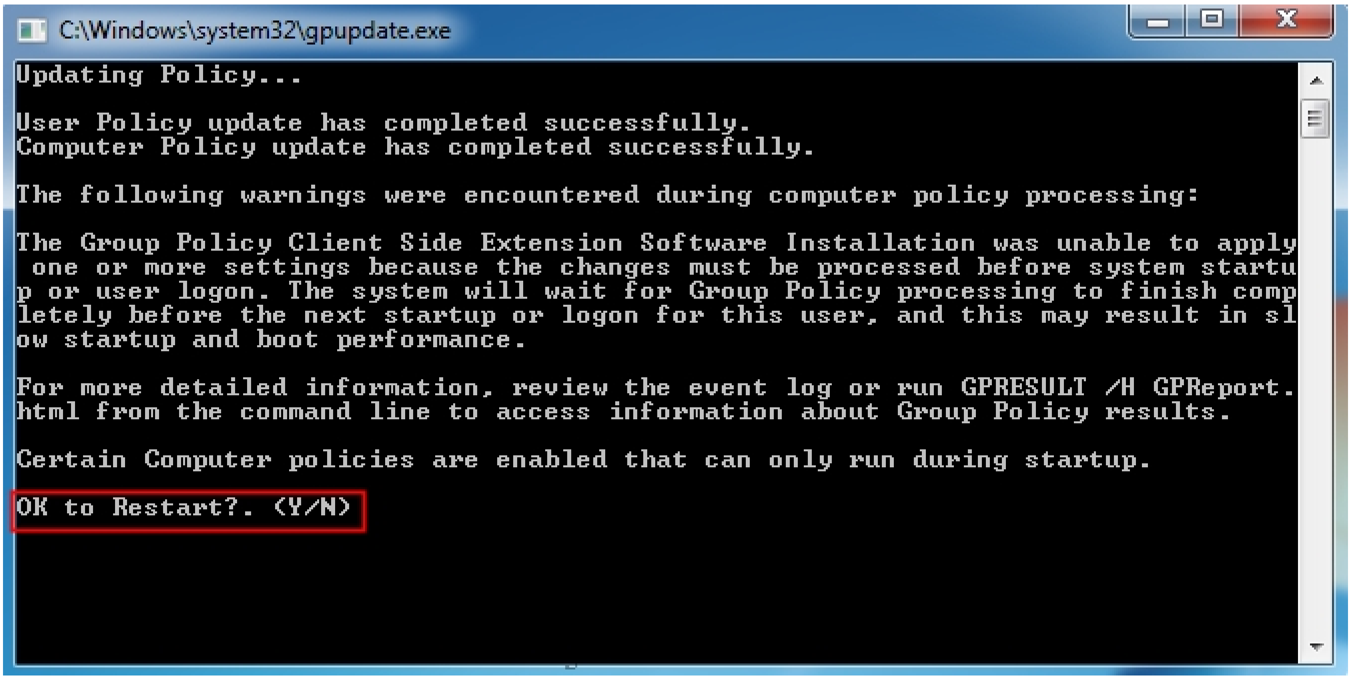
Windows Installer packages

You now see that LAPS x64 has been imported. In case you are adding x86 LAPS, once you add the package be sure to edit the x86 package to **uncheck** the option **Make this 32-bit X86 application available to Win64 machines**. You will find this option when you right click the x86 package > **Properties** > **Deployment**. This will ensure that 64-bit computers get the 64-bit DLL, and 32-bit machines get the 32-bit DLL. Close the GPM editor.



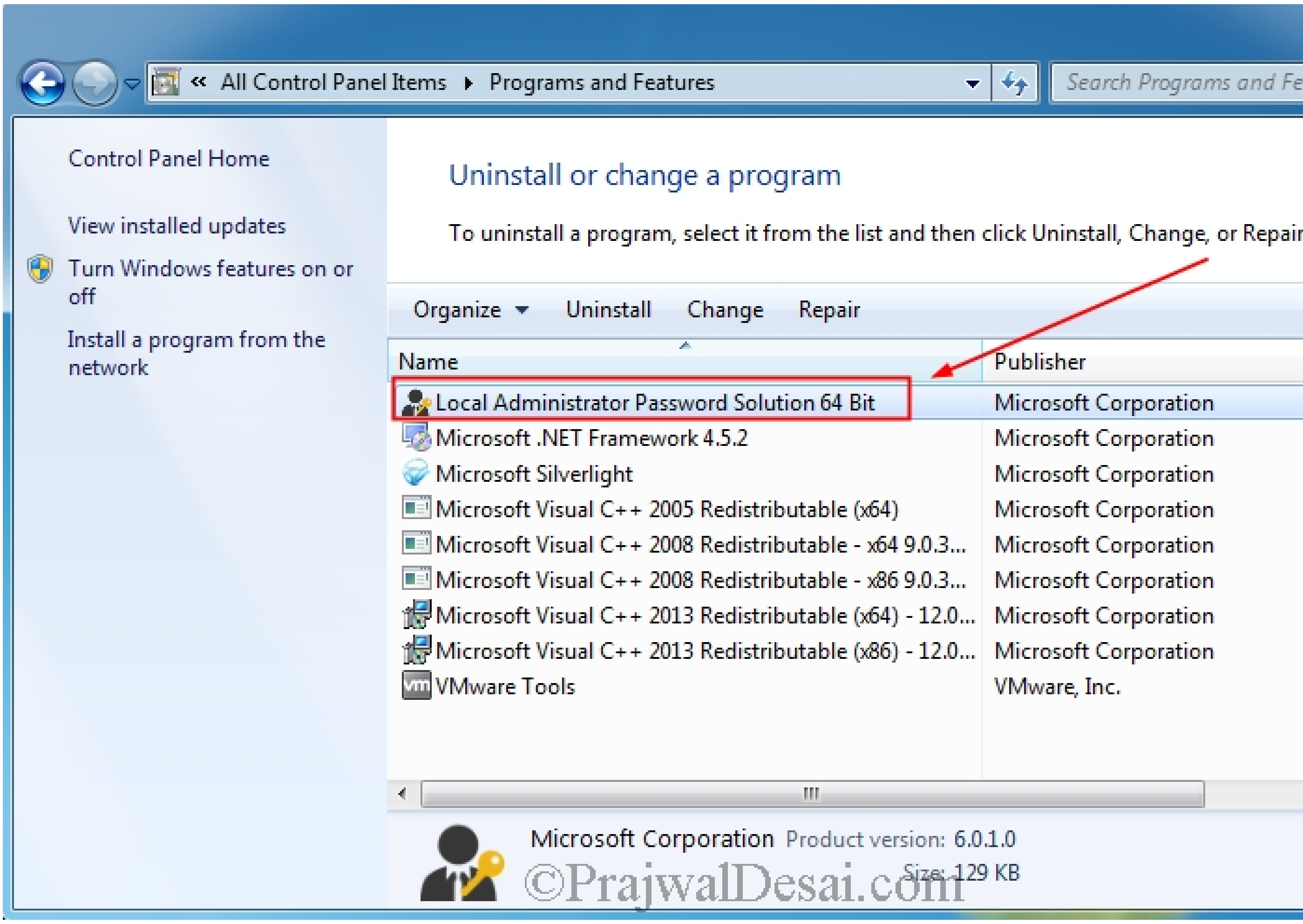
| Name | Versi... | Deployment st... | Source |
|---|---|---|---|
| Local Administrator Password Solution 6... | 6.0 | Assigned | \\ad\LAPS\LAPS.x64.msi |

To update the policy on the client machines, run the gpupdate command.



```
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply
 one or more settings because the changes must be processed before system startu
p or user logon. The system will wait for Group Policy processing to finish comp
letely before the next startup or logon for this user, and this may result in sl
ow startup and boot performance.

For more detailed information, review the event log or run GPRESULT /H GPReport.
html from the command line to access information about Group Policy results.

Certain Computer policies are enabled that can only run during startup.

OK to Restart?. (Y/N)
```

On the client machine launch the control panel and click on Program and Features. You will see that LAPS is installed on the client machine.



« All Control Panel Items ▸ Programs and Features
Search Programs and Fe
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize ▾
Uninstall
Change
Repair

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair

| Name | Publisher |
|---|---|
| Local Administrator Password Solution 64 Bit | Microsoft Corporation |
| Microsoft .NET Framework 4.5.2 | Microsoft Corporation |
| Microsoft Silverlight | Microsoft Corporation |
| Microsoft Visual C++ 2005 Redistributable (x64) | Microsoft Corporation |
| Microsoft Visual C++ 2008 Redistributable - x64 9.0.3... | Microsoft Corporation |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.3... | Microsoft Corporation |
| Microsoft Visual C++ 2013 Redistributable (x64) - 12.0... | Microsoft Corporation |
| Microsoft Visual C++ 2013 Redistributable (x86) - 12.0... | Microsoft Corporation |
| VMware Tools | VMware, Inc. |

Microsoft Corporation Product version: 6.0.1.0
Size: 129 KB

## How to configure Active directory for LAPS

Let’s see how to configure Active Directory for LAPS. We will first extend the AD Schema. Ensure that the user account that you use for this process should be a member of **Schema Admins** Active Directory group. The Active Directory Schema needs to be extended by two new attributes that store the password of the managed local Administrator account for each computer and the timestamp of password expiration. Both attributes are added to the may-contain attribute set of the computer class.

**ms-Mcs-AdmPwd** – Stores the password in clear text

**ms-Mcs-AdmPwdExpirationTime** – Stores the time to reset the password

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

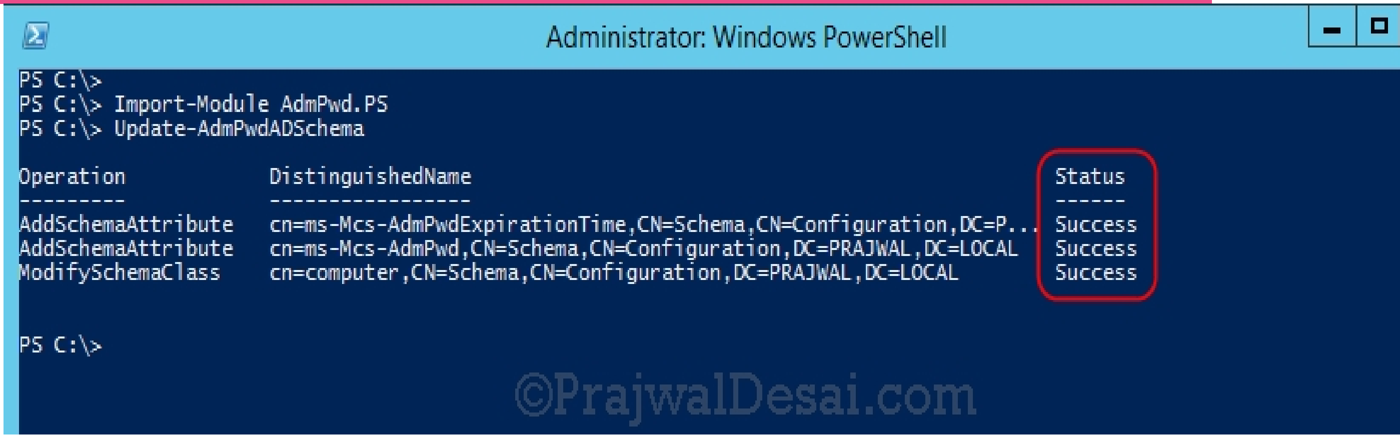
**Import-module AdmPwd.PS**

**Update-AdmPwdADSchema** (This command updates the schema)

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

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

Note – If you have an RODC installed in the environment and you need to replicate the value of the attribute ms-Mcs-AdmPwd to the RODC, you will need to change the 10th bit of the searchFlags attribute value for ms-Mcs-AdmPwd schema objet to 0 (substract 512 from the current value of the searchFlags attribute). For more information on Adding Attributes to or Removing attributes from the RODC Filtered Attribute Set, please refer to [http://technet.microsoft.com/en-us/library/cc754794(v=WS.10).aspx](http://technet.microsoft.com/en-us/library/cc754794(v=WS.10).aspx).

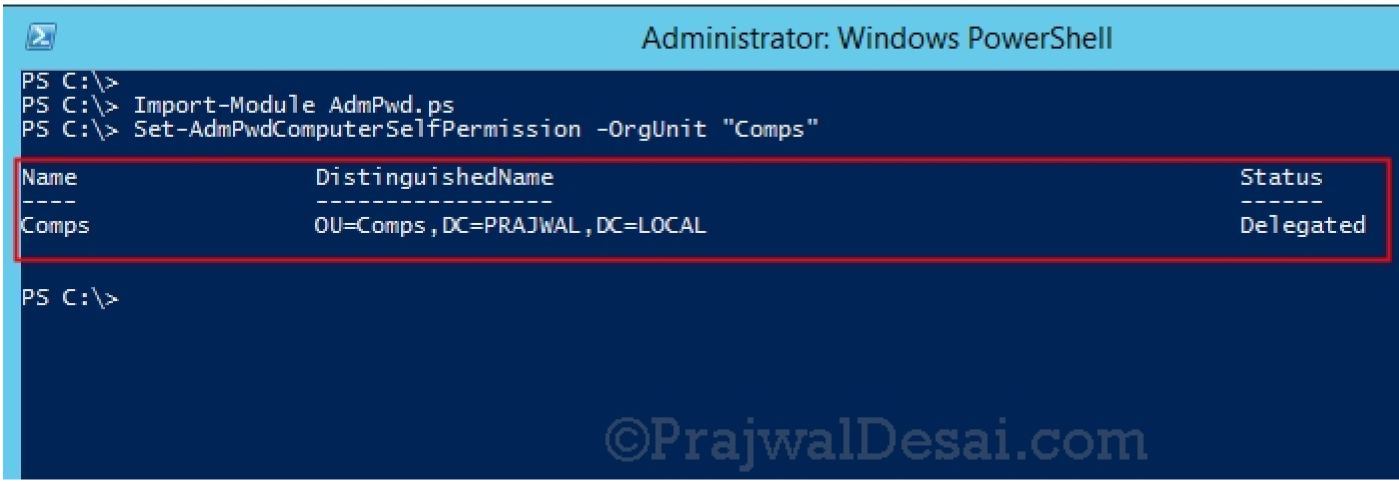


```
PS C:\>
PS C:\> Import-Module AdmPwd.PS
PS C:\> Update-AdmPwdADSchema

Operation           DistinguishedName                                           Status
---------           -----------------                                           ------
AddSchemaAttribute  cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=P... Success
AddSchemaAttribute  cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=PRAJWAL,DC=LOCAL   Success
ModifySchemaClass   cn=computer,CN=Schema,CN=Configuration,DC=PRAJWAL,DC=LOCAL        Success


PS C:\>
```

In the next step we will grant computers the ability to update their password attribute using the **Set-AdmPwdComputerSelfPermission** command. In this example I have got the client computers in “Comps OU”.  The Write permission on the **ms-Mcs-AdmPwdExpirationTime** and **ms-Mcs-AdmPwd** attributes of all computer accounts has to be added to the SELF built-in account. This is required so the machine can update the password and expiration timestamp of its own managed local Administrator password.  This is done using PowerShell.  You may need to run Import-module AdmPwd.PS if this is a new window.

**Set-AdmPwdComputerSelfPermission -OrgUnit <name of the OU to delegate permissions>**

Repeat this procedure for any additional OUs that contain computer accounts.



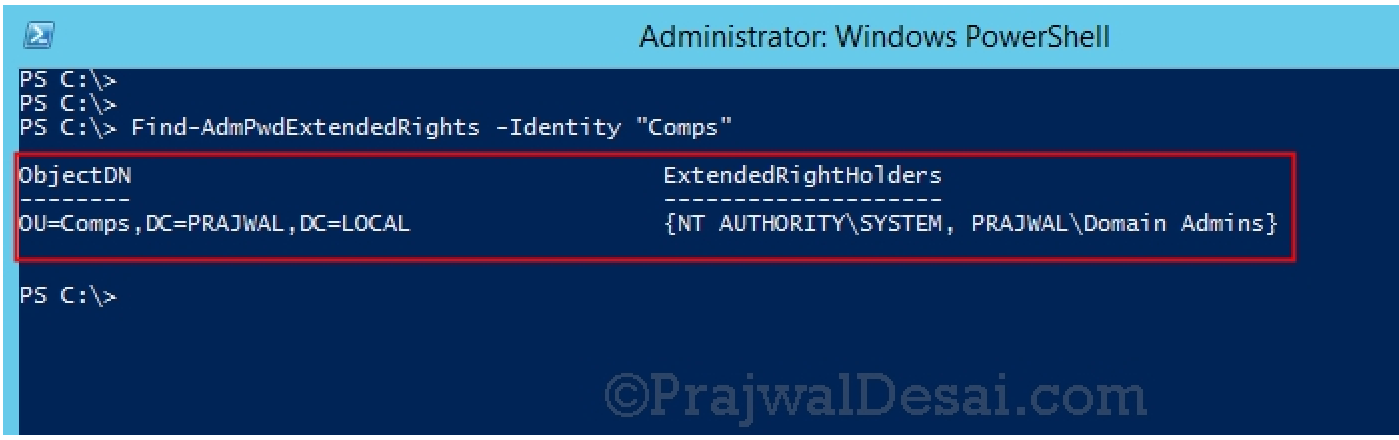
```
PS C:\>
PS C:\> Import-Module AdmPwd.ps
PS C:\> Set-AdmPwdComputerSelfPermission -OrgUnit "Comps"

Name                 DistinguishedName                                      Status
----                 -----------------                                      ------
Comps                OU=Comps,DC=PRAJWAL,DC=LOCAL                           Delegated

PS C:\>
```

**Removing the extended rights** – To restrict the ability to view the password to specific users and groups you need to remove "All extended rights" from users and groups that are not allowed to read the value of attribute ms-Mcs-AdmPwd. This is required because the All Extended rights/permissions permission also gives permission to read confidential attributes. If you want to do this for all computers you will need to repeat the next steps on each OU that contains those computers. You do not need to do this on subcontainers of already processed OUs unless you have disabled permission inheritance.

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.

To quickly find which security principals have extended rights to the OU you can use PowerShell cmdlet.  You may need to run **Import-module AdmPwd.PS** if this is a new window.

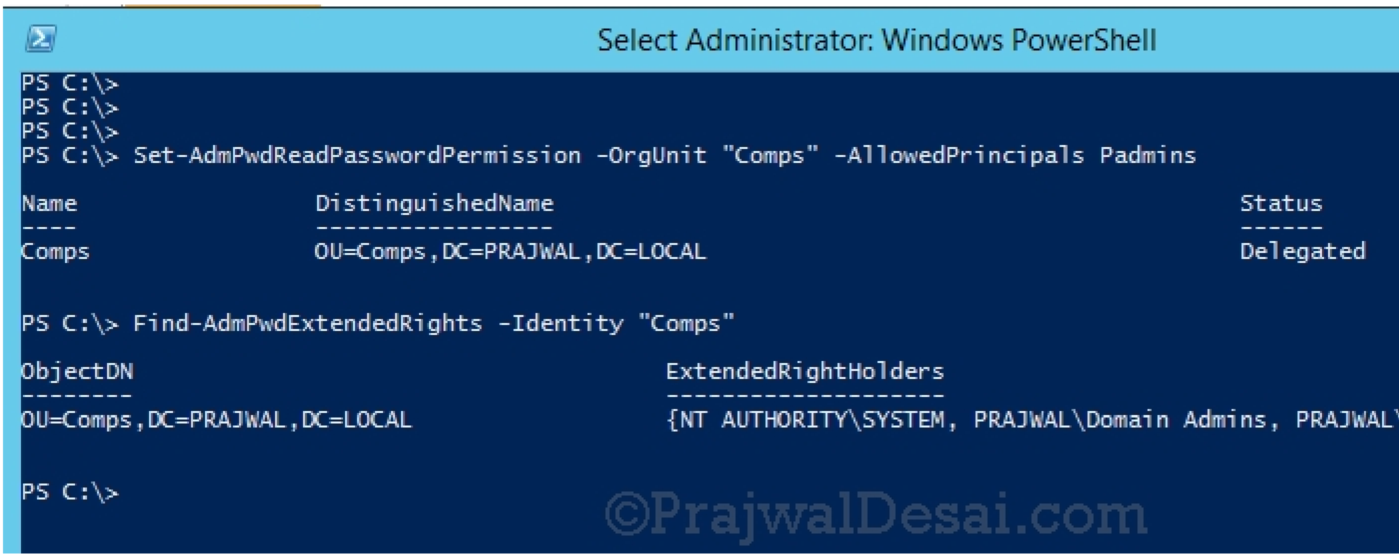
**Find-AdmPwdExtendedrights -identity "OU NAME"**



```
PS C:\>
PS C:\>
PS C:\> Find-AdmPwdExtendedRights -Identity "Comps"

ObjectDN                                    ExtendedRightHolders
--------                                    --------------------
OU=Comps,DC=PRAJWAL,DC=LOCAL                {NT AUTHORITY\SYSTEM, PRAJWAL\Domain Admins}

PS C:\>
```

In the next step we will grant rights to users to allow them to retrieve a computer’s password. We will use **Set-AdmPwdReadPasswordPermission** command to do this.

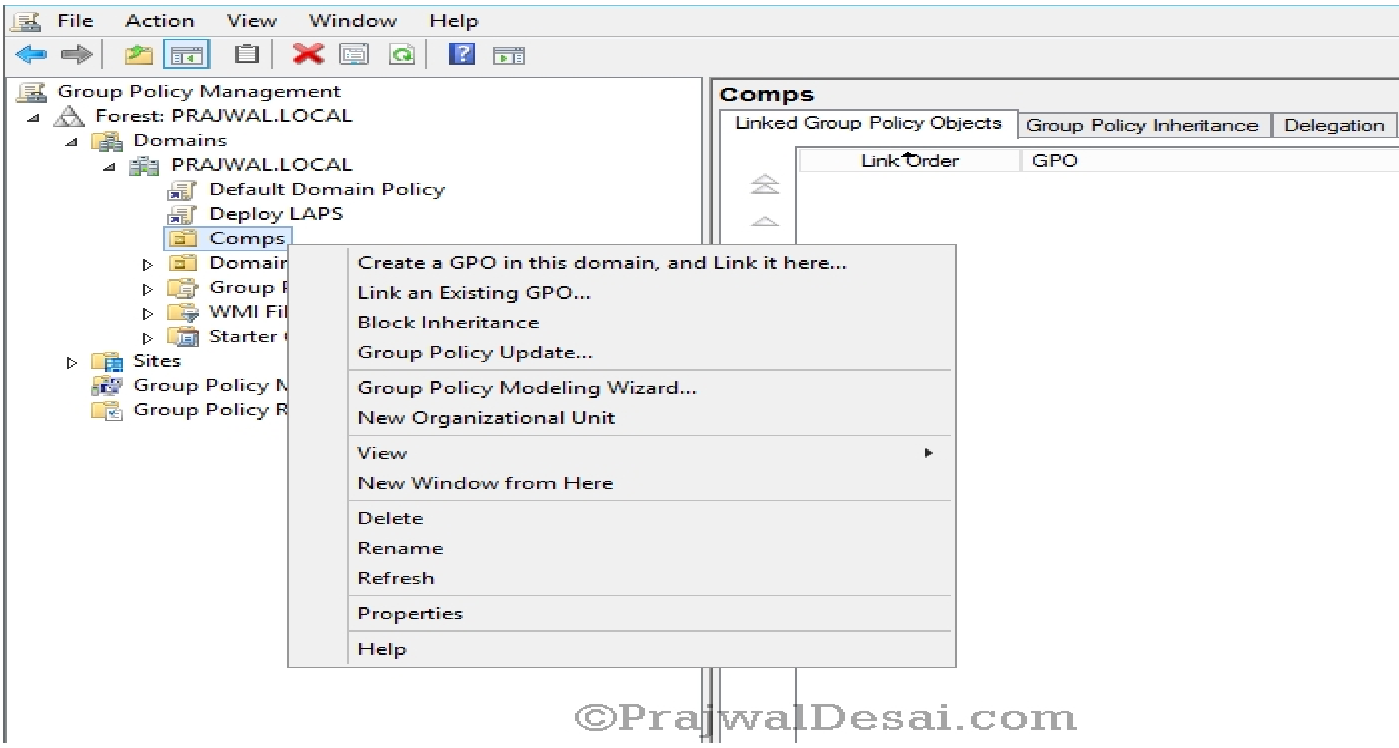
**Set-AdmPwdReadPasswordPermission -OrgUnit <name of the OU to delegate permissions> -AllowedPrincipals <users or groups>**



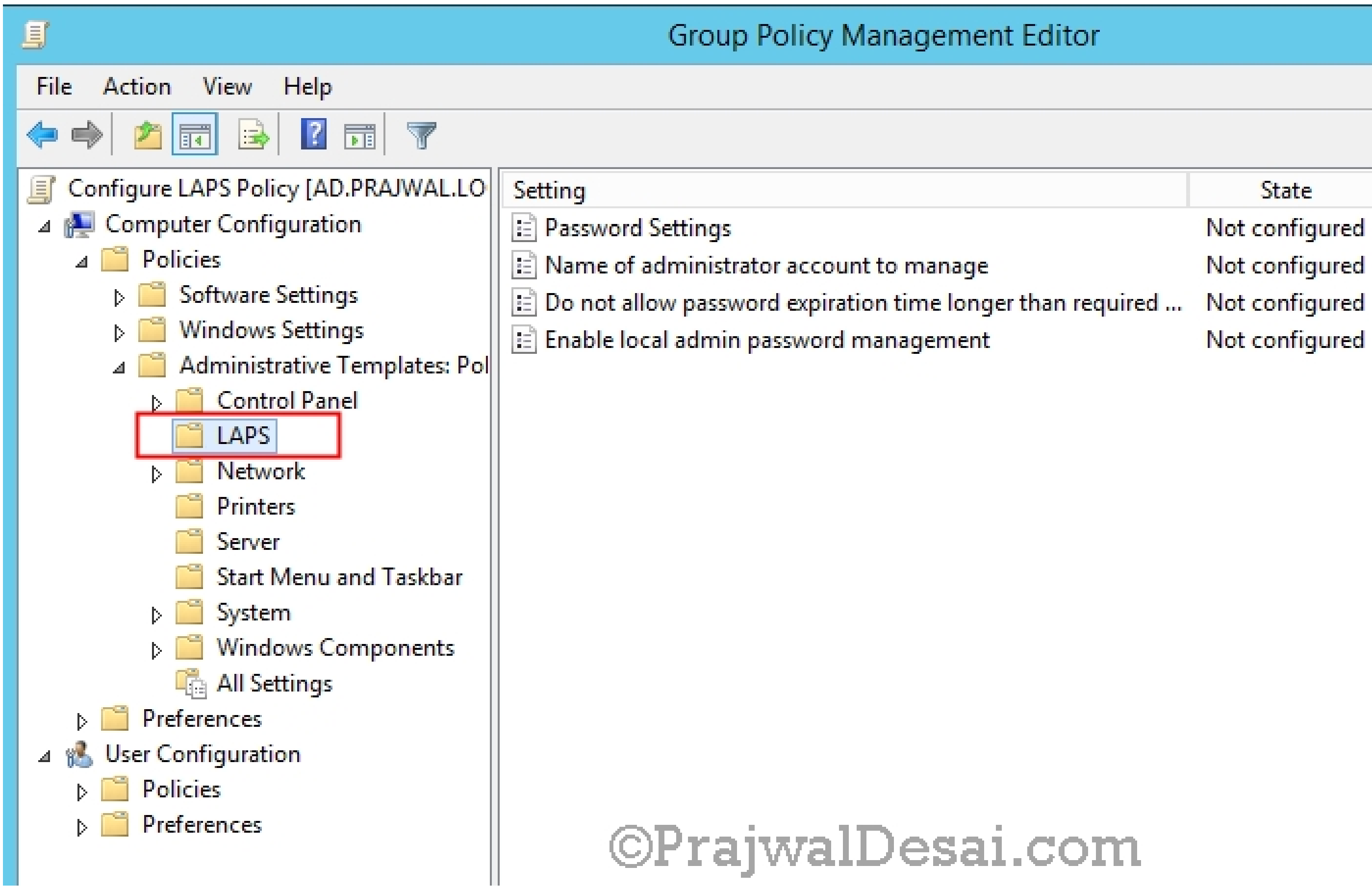
```
PS C:\>
PS C:\>
PS C:\>
PS C:\> Set-AdmPwdReadPasswordPermission -OrgUnit "Comps" -AllowedPrincipals Padmins

Name                DistinguishedName                                           Status
----                -----------------                                           ------
Comps               OU=Comps,DC=PRAJWAL,DC=LOCAL                                Delegated


PS C:\> Find-AdmPwdExtendedRights -Identity "Comps"

ObjectDN                                    ExtendedRightHolders
--------                                    --------------------
OU=Comps,DC=PRAJWAL,DC=LOCAL                {NT AUTHORITY\SYSTEM, PRAJWAL\Domain Admins, PRAJWAL\


PS C:\>
```

## How to configure Group Policy for LAPS

Launch the Group Policy Management console. I prefer to create a new policy to apply the password settings. Right click on the OU where your domain computers are present and click on Create a GPO in this domain and link it here. Specify a name to this GPO and click OK. Next, edit the GPO.

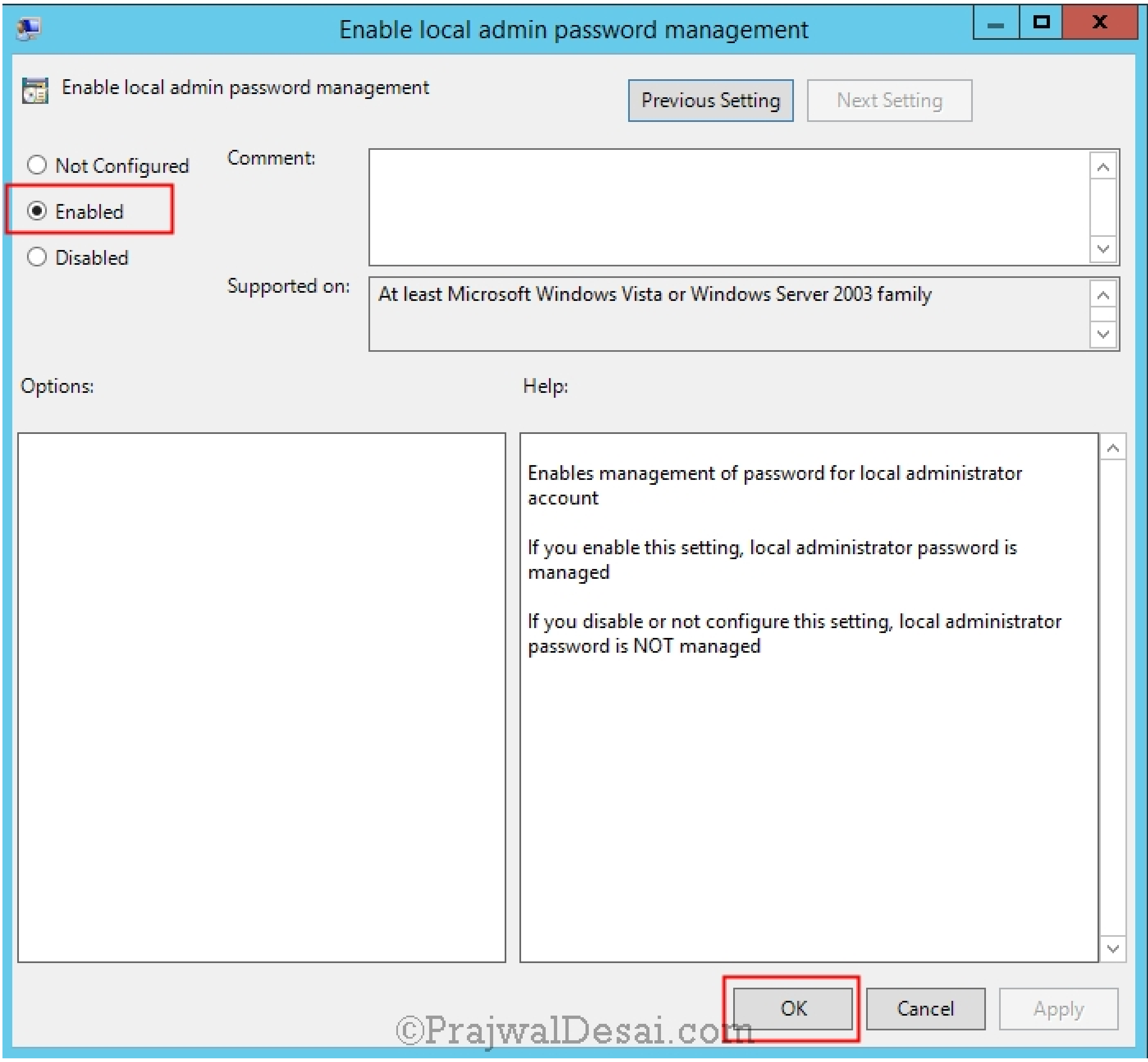


The settings are located under Computer Configuration > Administrative Templates > LAPS. You can see that there are 4 settings present. We will configure the ones that are required.



| Setting | State |
|---|---|
| Password Settings | Not configured |
| Name of administrator account to manage | Not configured |
| Do not allow password expiration time longer than required ... | Not configured |
| Enable local admin password management | Not configured |

Right click on the policy setting **Enable local admin password management** and click **properties**. As we want to manage the local administrator password, we will enable the policy setting. Click OK.



Enable local admin password management
Enable local admin password management
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured

● Enabled

○ Disabled

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

Enables management of password for local administrator account

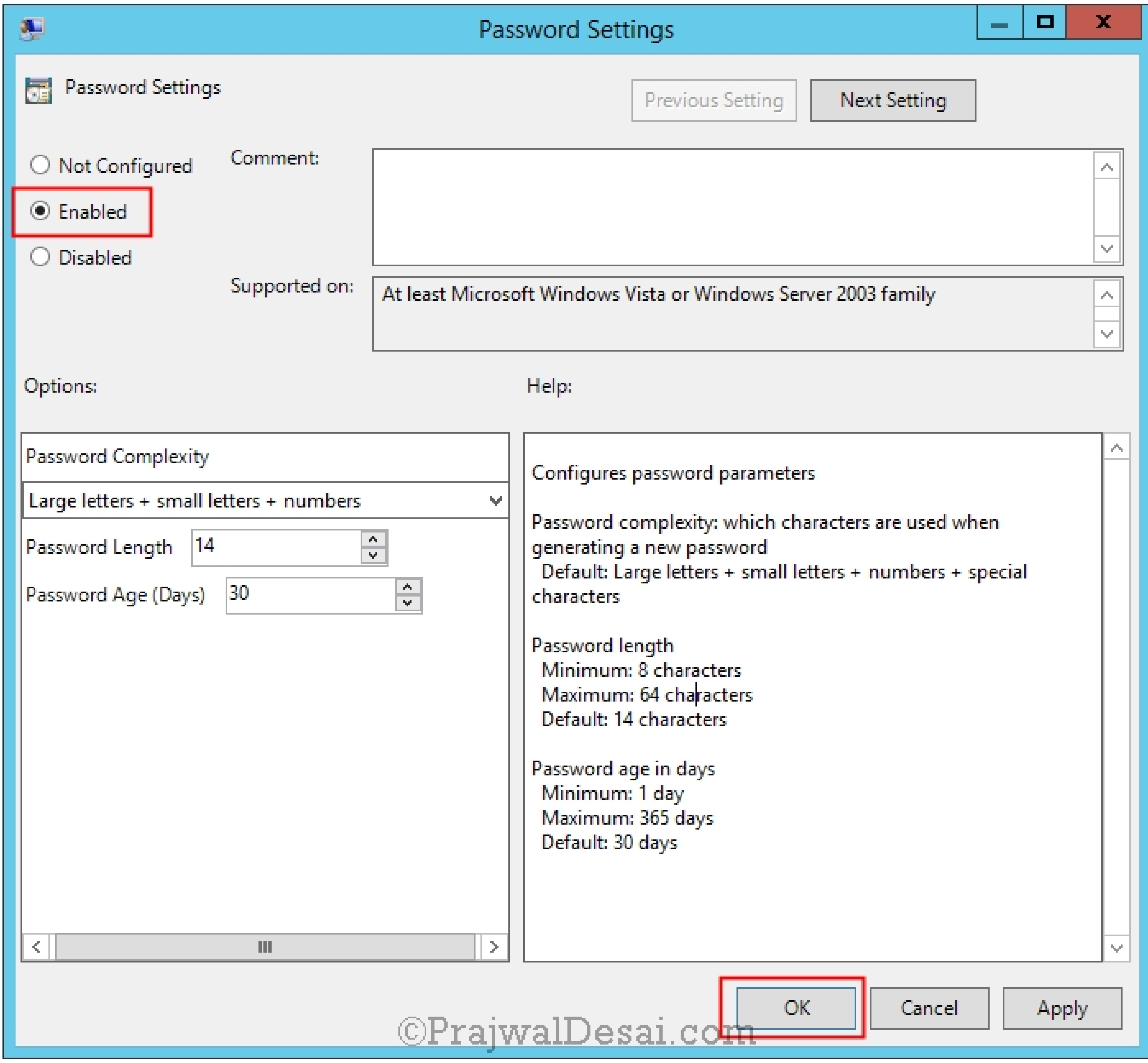
If you enable this setting, local administrator password is managed

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

The second policy setting that we will be enabling will be password settings. By default this solution uses a password with maximum password complexity, 14 characters and changes the password every 30 days. You can change the values to suit your needs by editing a Group Policy. You can change the individual password settings to fit your needs. Click OK.

**Administrator account name** – If you have decided to manage custom local Administrator account, you must specify its name in Group Policy. I have not configured this policy setting.

**Protection against too long planned time for password reset** – If you do not want to allow setting planning password expiration of admin account for longer time than maximum password age, you can do it in GPO.



● Enabled

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

Password Complexity: Large letters + small letters + numbers

Password Length: 14

Password Age (Days): 30

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

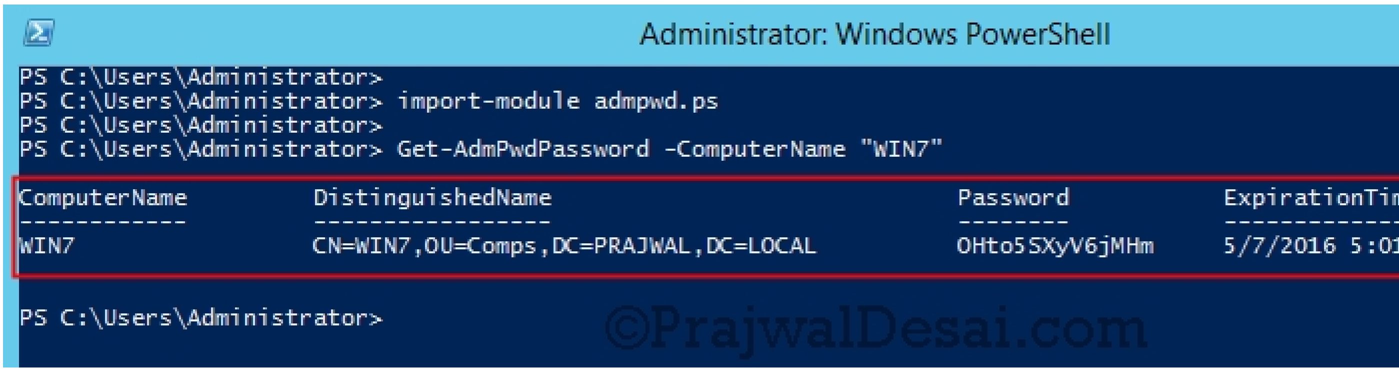
Password age in days
Minimum: 1 day
Maximum: 365 days
Default: 30 days

If you want to view the password settings of a computer using the powershell, Get-AdmPwdPassword will help you.

**Import-Module AdmPwd.PS**

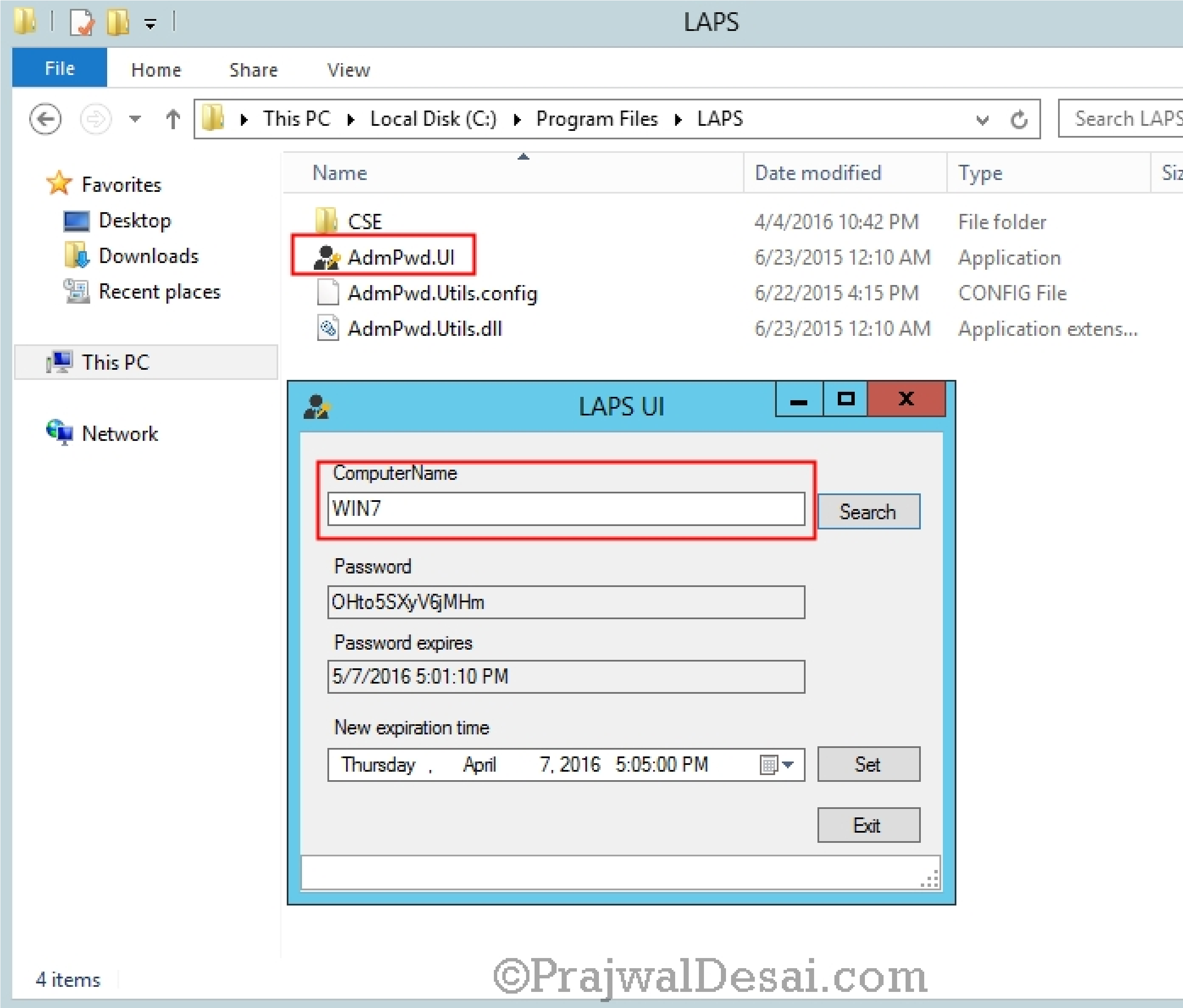
**Get-AdmPwdPassword -Computername “*name of computer*“**

What happens if a user who hasn’t been granted rights to see the local Administrators password tries to access it? If they were to gain access to the GUI interface the password won’t be displayed.



```
PS C:\Users\Administrator>
PS C:\Users\Administrator> import-module admpwd.ps
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-AdmPwdPassword -ComputerName "WIN7"

ComputerName          DistinguishedName                      Password           ExpirationTi
------------          -----------------                      --------           ------------
WIN7                  CN=WIN7,OU=Comps,DC=PRAJWAL,DC=LOCAL   OHto5SXyV6jMHm     5/7/2016 5:01

PS C:\Users\Administrator>
```

For GUI users there is a cool way to find the password settings. Run the **AdmPwd.UI** file as administrator. This file is located under C drive > Program Files > LAPS folder. In the LAPS UI window, enter the computer name and click **Search**. The password is shown and with expiry information.



| Name | Date modified | Type | Siz |
|---|---|---|---|
| CSE | 4/4/2016 10:42 PM | File folder | |
| AdmPwd.UI | 6/23/2015 12:10 AM | Application | |
| AdmPwd.Utils.config | 6/22/2015 4:15 PM | CONFIG File | |
| AdmPwd.Utils.dll | 6/23/2015 12:10 AM | Application extens... | |

LAPS UI

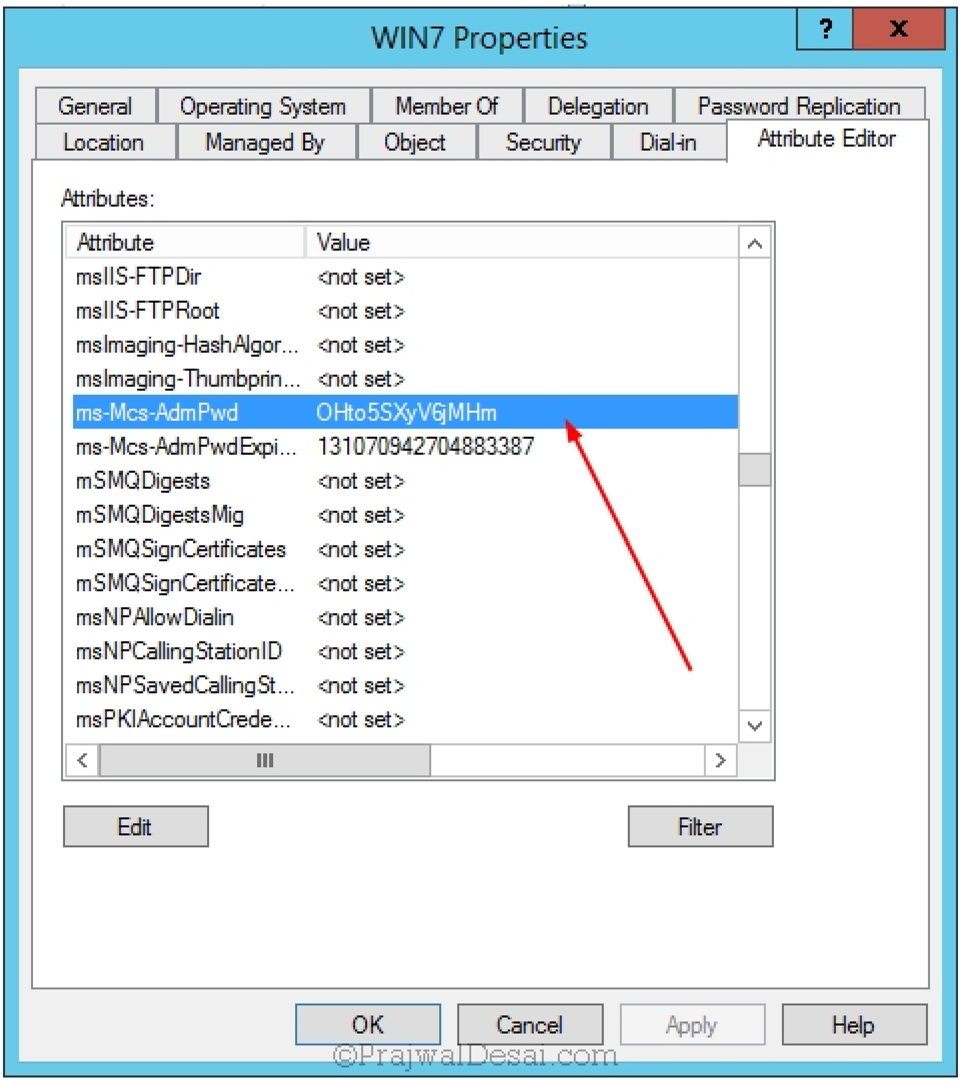
ComputerName: WIN7

Password: OHto5SXyV6jMHm

Password expires: 5/7/2016 5:01:10 PM

New expiration time: Thursday , April 7, 2016 5:05:00 PM

Once everything is configured, and Group Policy has refreshed on the clients, you can look at the properties of the computer object and see the new settings. The password is stored in plain text.



| Attribute | Value |
|---|---|
| msIIS-FTPDir | <not set> |
| msIIS-FTPRoot | <not set> |
| msImaging-HashAlgor... | <not set> |
| msImaging-Thumbprin... | <not set> |
| ms-Mcs-AdmPwd | OHto5SXyV6jMHm |
| ms-Mcs-AdmPwdExpi... | 131070942704883387 |
| mSMQDigests | <not set> |
| mSMQDigestsMig | <not set> |
| mSMQSignCertificates | <not set> |
| mSMQSignCertificate... | <not set> |
| msNPAllowDialin | <not set> |
| msNPCallingStationID | <not set> |
| msNPSavedCallingSt... | <not set> |
| msPKIAccountCrede... | <not set> |