Microsoft Local Administrator Password Solution (LAPS)

adsecurity.org

Sean Metcalf

September 15, 2015

The Issue

The real problem with local accounts on a computer in an enterprise environment is that the term “local” is a misnomer. If 50 computers on a network have the local administrator account of “Administrator” and a password of “P@55w0rd1!”, first of all that’s a HORRIBLE password. Second of all and more to the point, if one of those computers is compromised, they will all be compromised. Windows is very helpful. So helpful that if you pass the local admin credentials to another computer with the same local credentials, access is granted as if you logged on with the target system credentials. Dump administrator credentials on one to get admin on all! The best way to mitigate this issue is to ensure every computer has a different local administrator account password that is long, complex, and random and that changes on a regular basis.

The earlier attempt to provide a method for regularly changing the local administrator password from Microsoft was less than ideal (see Group Policy Preferences password storage security issue). You should also never, ever use a script that includes a clear-text password to change the local admin password since these scripts tend to be placed in easily accessible locations like SYSVOL (to leverage Group Policy).

Even if you deploy LAPS or some other local Administrator account password management solution, it’s still recommended to install KB2871997 (if required) and configure a Group Policy to block local accounts from authenticating across the network. KB2871997 adds two new local SIDs including LOCAL_ACCOUNT_AND_MEMBER_OF_ADMINISTRATORS_GROUP (S-1-5-114) for any local account that is a member of the administrators group. Configuring this SID in a Group Policy with the settings “Deny access to this computer from the network” and “Deny log on through Remote Desktop Services” prevents local accounts from connecting over the network (for workstations, test carefully before deploying to servers).

I also posted about “Microsoft LAPS Security & Active Directory LAPS Configuration Recon” in August 2016 which covers some of the more interesting LAPS security scenarios.

Microsoft Local Administrator Password Solution (LAPS) Overview

Microsoft Local Administrator Password Solution (LAPS) provides automated local administrator account management for every computer in Active Directory (LAPS is best for workstation local admin passwords). A client-side component installed on every computer generates a random password, updates the (new) LAPS password attribute on the associated AD computer account, and sets the password locally. LAPS configuration is managed through Group Policy which provides the values for password complexity, password length, local account name for password change, password change frequency, etc.

Microsoft Local Administrator Password Solution (LAPS):

> For environments in which users are required to log on to computers without domain credentials, password management can become a complex issue. Such environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack. 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.
>
> LAPS simplifies password management while helping customers implement recommended defenses against cyberattacks. In particular, the solution mitigates the risk of lateral escalation that results when customers use the same administrative local account and password combination on their computers. LAPS stores the password for each computer's local administrator account in Active Directory, secured in a confidential attribute in the computer's corresponding Active Directory object. The computer is allowed to update its own password data in Active Directory, and domain administrators can grant read access to authorized users or groups, such as workstation helpdesk administrators.
>
> Use LAPS to automatically manage local administrator passwords on domain joined computers so that passwords are unique on each managed computer, randomly generated, and securely stored in Active Directory infrastructure. The solution is built on Active Directory infrastructure and does not require other supporting technologies. LAPS uses a Group Policy client-side extension (CSE) that you install on managed computers to perform all management tasks. The solution's management tools provide easy configuration and administration.
>
> **How does LAPS work?**
> The core of the LAPS solution is a GPO client-side extension (CSE) that performs the following tasks and can enforce the following actions during a GPO update:
> • Checks whether the password of the local Administrator account has expired.
> • Generates a new password when the old password is either expired or is required to be changed prior to expiration.
> • Validates the new password against the password policy.
> • Reports the password to Active Directory, storing it with a confidential attribute with the computer account in Active Directory.
> • Reports the next expiration time for the password to Active Directory, storing it with an attribute with the computer account in Active Directory.
> • Changes the password of the Administrator account.
> The password then can be read from Active Directory by users who are allowed to do so. Eligible users can request a password change for a computer.
>
> **What are the features of LAPS?**
> LAPS includes the following features:
> • Security that provides the ability to:

> • Randomly generate passwords that are automatically changed on managed machines.
> • Effectively mitigate PtH attacks that rely on identical local account passwords.
> • Enforced password protection during transport via encryption using the Kerberos version 5 protocol.
> • Use access control lists (ACLs) to protect passwords in Active Directory and easily implement a detailed security model.
> • Manageability that provides the ability to:
> • Configure password parameters, including age, complexity, and length.
> • Force password reset on a per-machine basis.
> • Use a security model that is integrated with ACLs in Active Directory.
> • Use any Active Directory management tool of choice; custom tools, such as Windows PowerShell, are provided.
> • Protect against computer account deletion.
> • Easily implement the solution with a minimal footprint.

The Microsoft Security Advisory 3062591 includes additional information on LAPS.

Why is this important?

LAPS solves the difficult issue of managing every computer's local administrator account password which is often only used in situations where a domain account cannot. Often a local administrator account password will remain the same throughout the lifetime of a computer and is often the same as many other computers on the network. The same local administrator account and password on multiple computers can be exploited by attackers to compromise a network. Ensuring local admin account passwords are different on every computer on the network mitigates an attackers ability to expand administrative control beyond a single system using local credentials.

How is it configured?

LAPS deployment has several steps:

1. Download LAPS files...This includes the Operations guide – please read it thoroughly before deploying
2. Active Directory schema update to add the 2 required LAPS attributes for computer accounts.
3. Delegation at the domain or Organizational Unit (OU) level so the computers can update their LAPS passwords.
4. Delegation at the OU level enabling AD groups to view or force a reset of computer local admin account passwords.
5. Installation of the LAPS client-side component (via SCCM or similar) which performs the password change and updates the computer's attribute based on LAPS GPO settings.
6. A new Group Policy created to enable the LAPS client-side component to change the local account password as well as provide LAPS configuration for the client (password complexity, password length, local account name for password change, password change frequency, etc).

Once LAPS is deployed, there are several methods approved users can view the computer local admin password(s):

- PowerShell:
  Get-AdmPwdPassword -ComputerName <computername>
- Active Directory Users & Computers:
  View the value of the computer attribute ms-Mcs-AdmPwd
- LAPS Client

Pros:

- Fully automated, configurable computer local administrator account updating
- Simple delegation for access to stored passwords by OU.
- No need for additional servers since LAPS leverages Active Directory components (Group Policy, computer object attributes, etc).
- Computer account can only write/update its own local Administrator account password (ms-Mcs-AdmPwd attribute), it can’t read the password from the attribute.
- Password update traffic is encrypted.
- Password changes for every computer in an OU/domain can be performed easily. (blank out password last set attribute)
- Free (as in no cost for the software, your time & resources are extra)

Cons:

- Passwords are stored in clear-text and may be exposed if delegation is not properly planned/deployed. Note that encryption key management is hard and complicates solutions. Focus on proper delegation and this risk is mitigated.
- Only the current password is stored and available for retrieval.
- Only one local administrator account can have its password managed by LAPS at a time (only one password attribute)..
- Domain Controller compromise can compromise all local administrator account passwords in the domain.
- Passwords can be accessed at any point and used by those delegated to view them at any time. While there is auditing that can be enabled, it has to be configured per OU, per group which logs event ID 4662 on the Domain Controller. Additionally, the password is not automatically changed after use as in some other local account password management solutions.
- Extended rights may be configured in the environment which could allow unauthorized users to access LAPS passwords on some computers. Additional information on how to remove Extended rights is the in LAPS Operation Guide (and some of it is at the end of this post in the Delegation section.

LAPS enables password management of the local Administrator account (RID 500) password or another custom local account. Microsoft recommends that only the default Administrator local account is a member of the local Administrators group and that LAPS manages that account.

LAPS in a Virtual Environment:

LAPS works pretty well when configured on a physical computer that doesn't change state. Things get a little tricky when you introduce LAPS in a VDI environment.

Persistent VDI (same computer name):
This process is the same as a physical computer since the user connects to the same VDI image which persists (not destroyed at logoff).

Non-Persistent VDI (new computer name):
If the VDI workstation has a new computer name at every connect (non-persistent session, new computer image spun-up as part of user logon), then LAPS will update the password when the LAPS client runs and notices the ms-Mcs-AdmPwdExpirationTime attribute for the AD computer account is blank. As part of this process, the LAPS client generates and sets the local admin password and then updates the LAPS ms-Mcs-AdmPwd attribute on the AD Computer account (the ms-Mcs-AdmPwdExpirationTime attribute is updated as well). No problem here as this process is the same as a physical computer.

Non-Persistent VDI (same computer name:
If the VDI workstation has the same computer name at every connect (non-persistent session, same computer image spun-up), then LAPS will not update the password when the LAPS client runs soon after startup since it will notice that the ms-Mcs-AdmPwdExpirationTime attribute for the AD computer account is within the defined threshold (14 days for example). In this case the LAPS client will sleep until it notices the value in the ms-Mcs-AdmPwdExpirationTime attribute is greater than the threshold. This means that the VDI system would have the default VDI image password during most of the threshold period and for the time while the VDI system is active when the LAPS threshold is exceeded. At this point, LAPS updates the local administrator password locally and on the ms-Mcs-AdmPwdExpirationTime attribute on the AD computer account as well as the ms-Mcs-AdmPwdExpirationTime attribute at which point it sleeps for the defined number of days (14 in this case).
Since LAPS doesn't have an (obvious) option to force the LAPS client to change the password at boot-up, a script would need to run to clear the ms-Mcs-AdmPwdExpirationTime attribute so when the LAPS client runs (GPO refresh time) and checks the last password change time (ms-Mcs-AdmPwdExpirationTime), the local admin password would be changed. A PowerShell script can be configured that clears the ms-Mcs-AdmPwdExpirationTime when the user logs off (or during another event). The VDI solution may provide the ability to run a script at this point. A computer startup script (via GPO) would work as well.

Auditing Access:
Configure LAPS access auditing:

> Set-AdmPwdAuditing –OrgUnit: <name of OU on which you want to setup the auditing> -AuditedPrincipals: :<identification of users/groups whose access to password shall be audited>

When someone accesses the LAPS password attribute, event ID 4662 is logged on the Domain Controller that responded to the read request.

Notes:

- Since this solution is meant to automate the changing of local admin passwords as well as keeping this information private, identifying who should be able to retrieve the local admin passwords on a set of computers needs to be well thought-out.
- Key point is that delegation of (read) access to the password attribute needs to be carefully designed and deployed. This is the most important part of a LAPS deployment: determining who should have read access to the computer password data.
- The password itself should be about 25 characters (because that’s what is “reasonable” today). It should definitely be more than 15.
- The local admin password should also rotate at least as frequently as the computer AD account passwords (every 15 – 30 days).
- Accounts delegated to join computers to the domain may be able to view LAPS password data on computer objects.

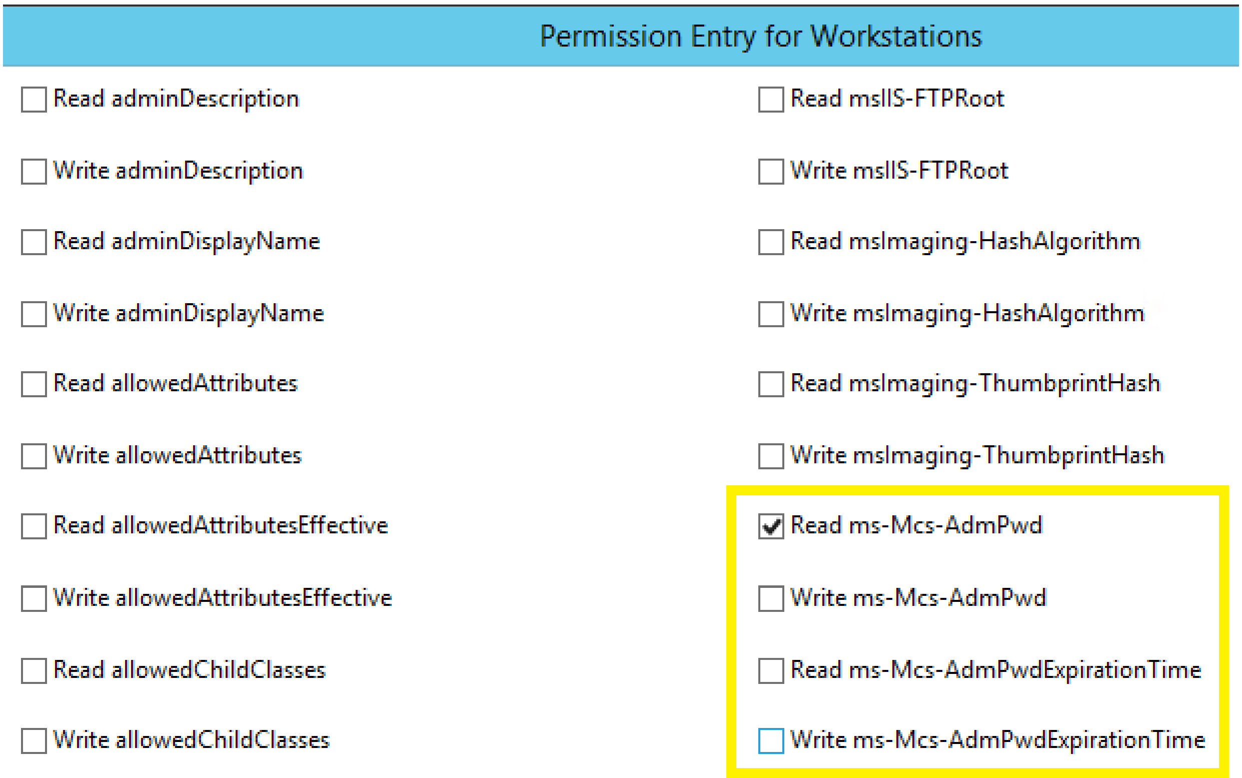
LAPS Enterprise (LAPS-E) Note:

There was another version of LAPS, known as LAPS Enterprise (LAPS-E), which included additional features such as encrypted passwords and management of multiple local accounts (if deployed as part of a customized Microsoft delivery). However, LAPS-E has a different code base from LAPS and hasn’t complete required security reviews within Microsoft. There is also no update model to ensure that customers receive code updates. Because of this, *Microsoft doesn’t support LAPS-E, and no longer includes LAPS-E in any customer deliverables.* This means you shouldn’t use LAPS-E (though the code is available on MSDN). In fact, LAPS works really well and if advanced functionality is required, there are several third-party products that provide similar capability and more (Cyber-Ark, Thycotic, Xceedium, Lieberman, Dell, etc).

LAPS Installation

LAPS requires updating the Active Directory schema, so membership in Schema Admins is required for at least part of the install.

Please read through the LAPS documentation (LAPS Operation Guide, etc) before installing as it will save you time and hassle.

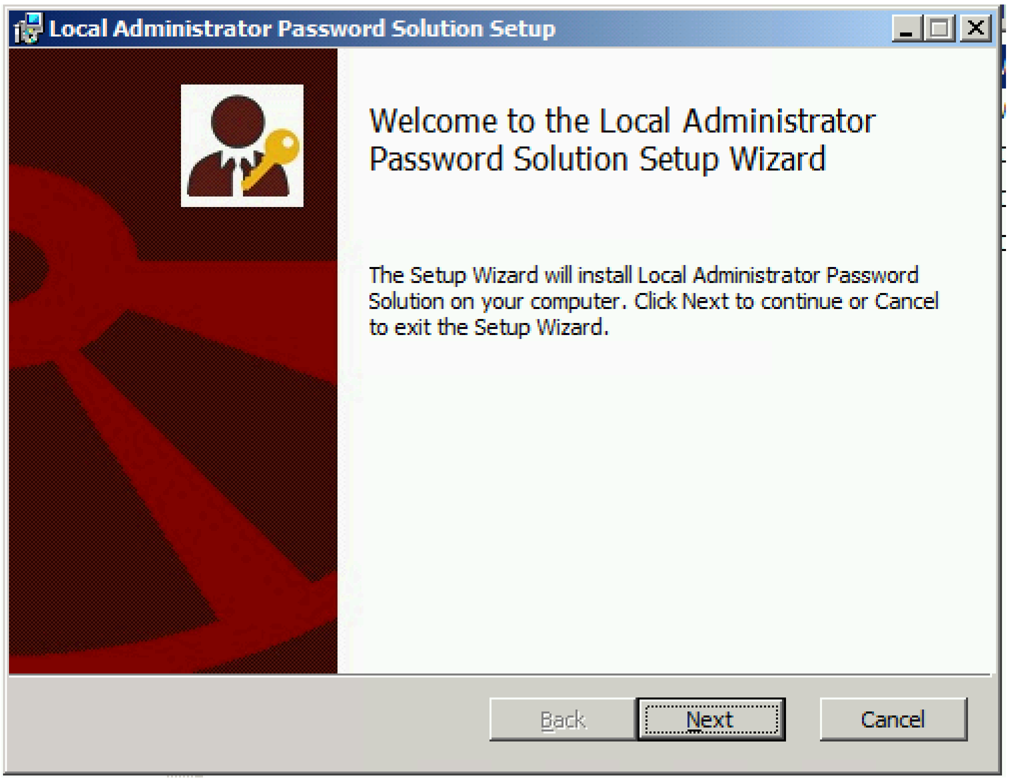


Permission Entry for Workstations

□ Read adminDescription
□ Write adminDescription
□ Read adminDisplayName
□ Write adminDisplayName
□ Read allowedAttributes
□ Write allowedAttributes
□ Read allowedAttributesEffective
□ Write allowedAttributesEffective
□ Read allowedChildClasses
□ Write allowedChildClasses

□ Read msIIS-FTPRoot
□ Write msIIS-FTPRoot
□ Read msImaging-HashAlgorithm
□ Write msImaging-HashAlgorithm
□ Read msImaging-ThumbprintHash
□ Write msImaging-ThumbprintHash
☑ Read ms-Mcs-AdmPwd
□ Write ms-Mcs-AdmPwd
□ Read ms-Mcs-AdmPwdExpirationTime
□ Write ms-Mcs-AdmPwdExpirationTime

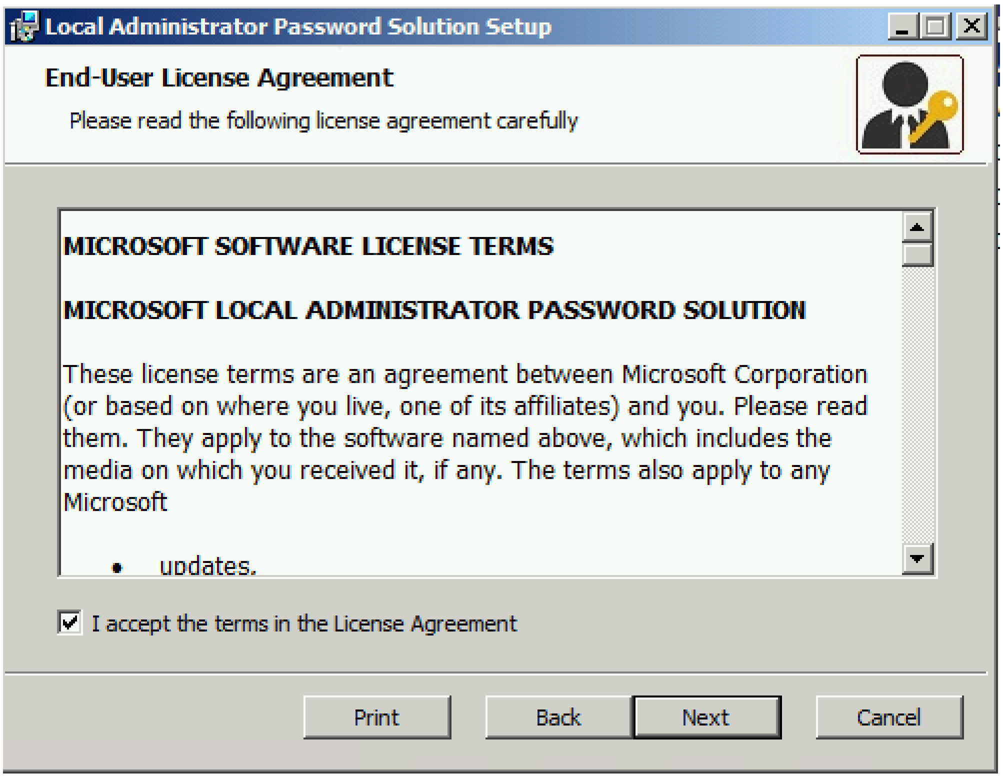
Start the install…



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.



End-User License Agreement

Please read the following license agreement carefully

MICROSOFT SOFTWARE LICENSE TERMS

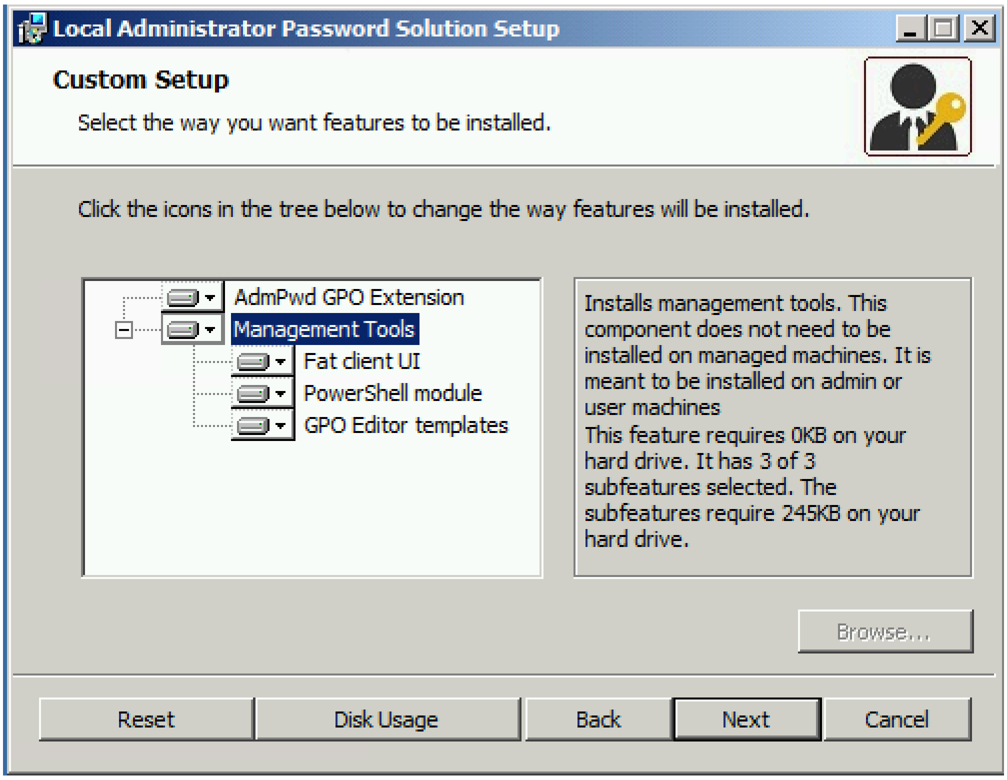
MICROSOFT LOCAL ADMINISTRATOR PASSWORD SOLUTION

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

The custom setup page has several options.
The Fat client UI & PowerShell module only need to be installed on systems which will manage LAPS which includes those who will access the password(s).
The GPO components are for deploying & managing the LAPS GPOs.



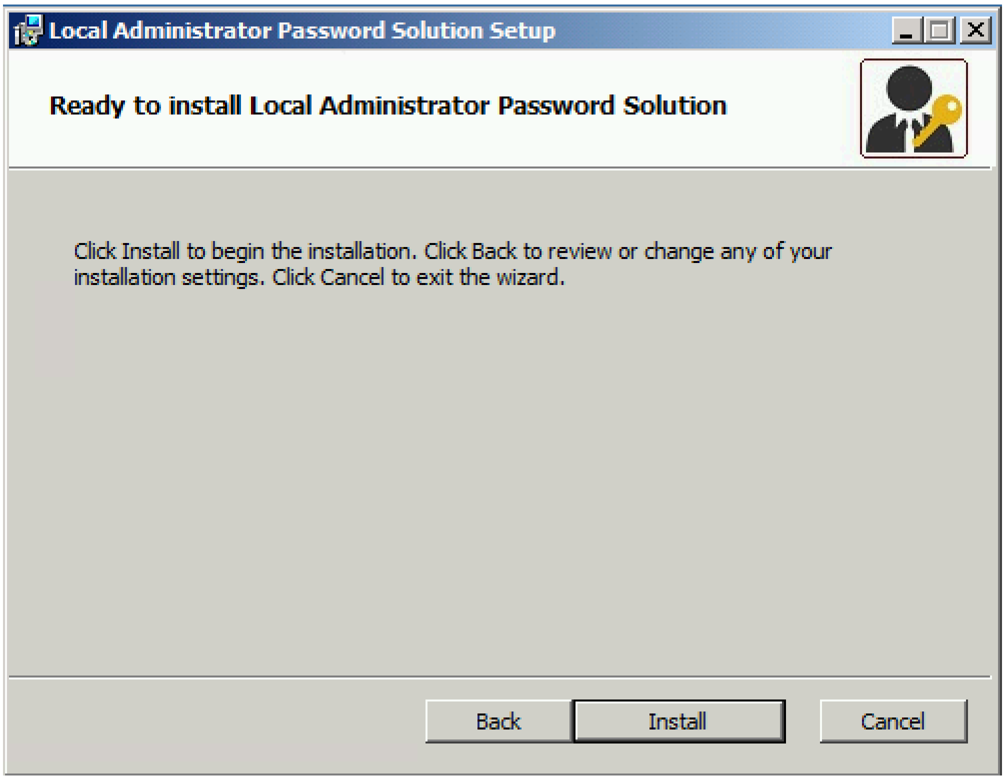
Custom Setup

Select the way you want features to be installed.

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

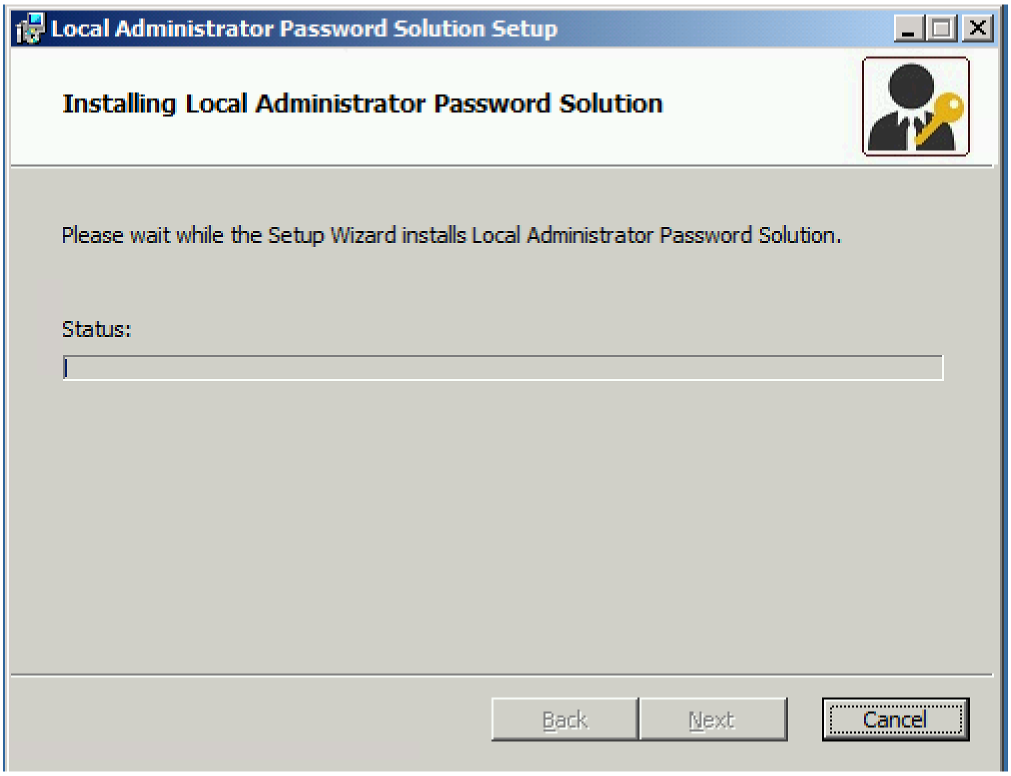
- AdmPwd GPO Extension
- Management Tools
  - Fat client UI
  - PowerShell module
  - GPO Editor templates

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 245KB on your hard drive.



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.



Installing Local Administrator Password Solution

Please wait while the Setup Wizard installs Local Administrator Password Solution.

Status:

Local Administrator Password Solution Setup

Completed the Local Administrator Password Solution Setup Wizard

Click the Finish button to exit the Setup Wizard.

NOTE:

Don’t install the LAPS client on a Domain Controller (and have the LAPS GPO configured at the domain level) since LAPS will start changing the default Administrator account (RID 500) for the domain. This happened to me in a lab environment and was fun tracking it down!

The LAPS client installed can be verified by checking for admpwd.dll in c:\program files\LAPS\CSE.

PowerShell is a quick & easy way to verify install: *Get-ChildItem ‘c:\program files\LAPS\CSE\Admpwd.dll’*

GPO Client Side Extensions (CSEs) are registered here:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions

The admpwd GPO CSE is registered in this location.

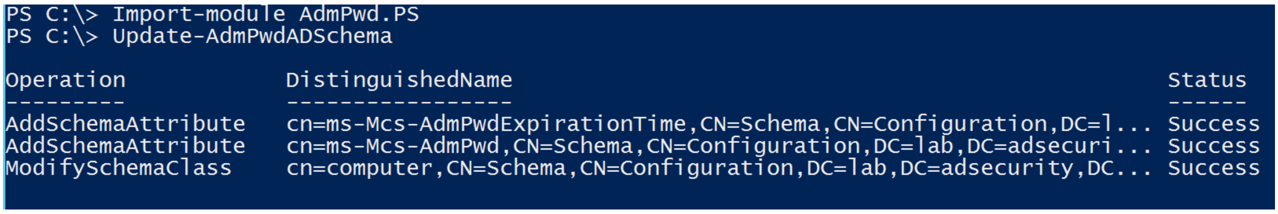
LAPS Schema Update

Once the LAPS client is installed and before any other configuration, now is a good time to extend the AD schema with the LAPS computer object attributes. Remember to always perform backups before modifying the AD schema.

The LAPS schema adds two attributes:

- ms-Mcs-AdmPwd – Stores the password in clear text
- ms-Mcs-AdmPwdExpirationTime – Stores the time to reset the password

LAPS includes a PowerShell cmdlet for updating the AD schema: Update-AdmPwdADSchma.



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

Operation           DistinguishedName                                                 Status
---------           -----------------                                                 ------
AddSchemaAttribute  cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=l... Success
AddSchemaAttribute  cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=lab,DC=adsecuri... Success
ModifySchemaClass   cn=computer,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC... Success
```

There is an important LAPS note when installing in an environment with RODCs:

> ***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.

Group Policy Configuration

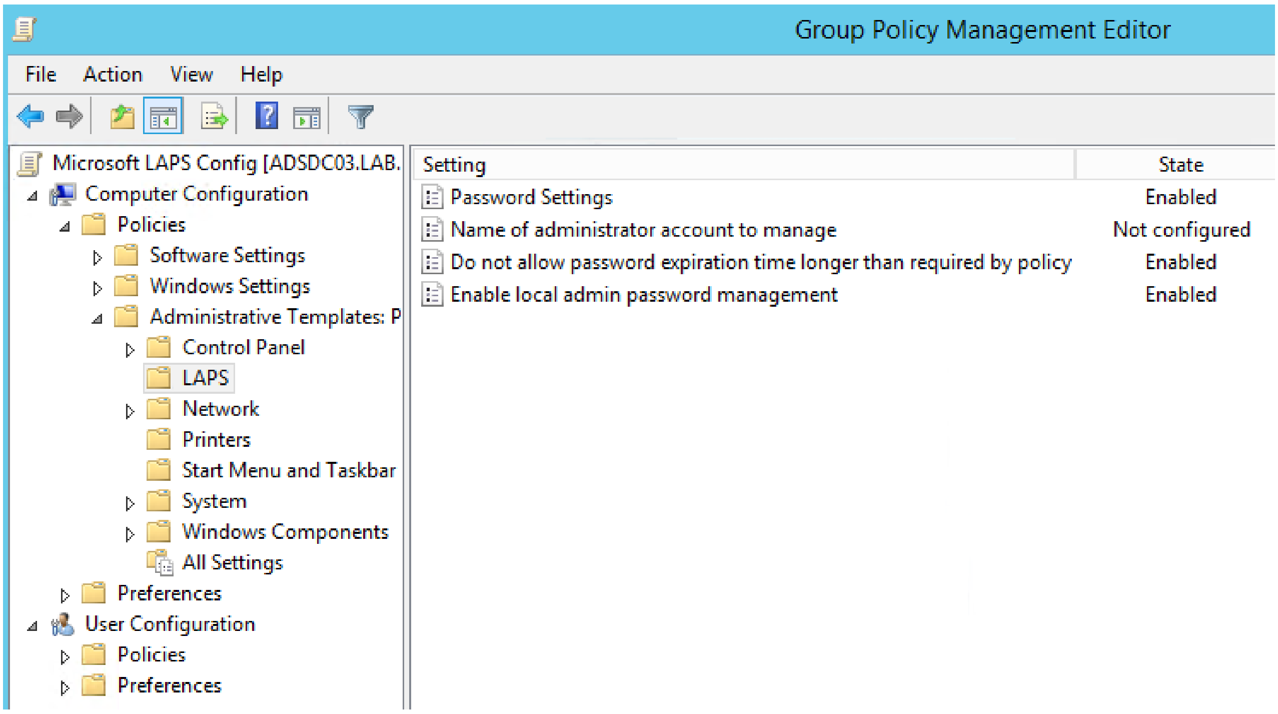
The LAPS Group Policy admin templates are copied to the local system when LAPS is installed:

- AdmPwd.admx –> %WINDIR%\PolicyDefinitions
- AdmPwd.adml –> %WINDIR%\PolicyDefinitions\en-US

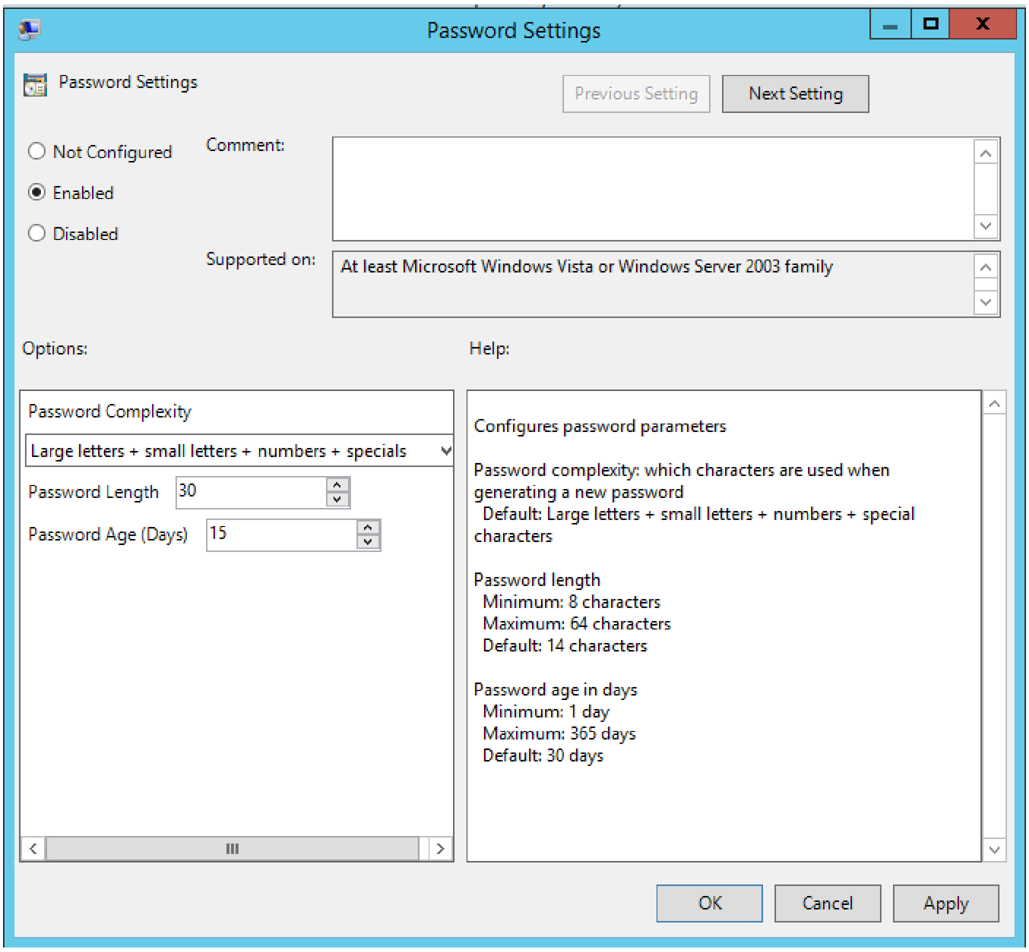
These files can be copied to the AD GPO Central Store so LAPS GPOs can be managed from any system (admx files in the PolicyDefinitions and the adml file in the en-US sub-folder).

There are four primary LAPS configuration settings:

1. Password Settings – configure password length & complexity.
2. Configure if there's an account other than the default Administrator account (RID 500).
3. Enable this to prevent local admin passwords from being older than the domain password policy (set to Enabled). More on this in my LAPS security post.
4. Enable to enable LAPS to manage the local admin password. Don't switch to "Enabled" until you are ready to have LAPS manage the passwords. If this is not Enabled, the LAPS client will not manage the passwords.



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



○ Not Configured
● Enabled
○ Disabled

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

Password Complexity: Large letters + small letters + numbers + specials

Password Length: 30

Password Age (Days): 15

Configures password parameters

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

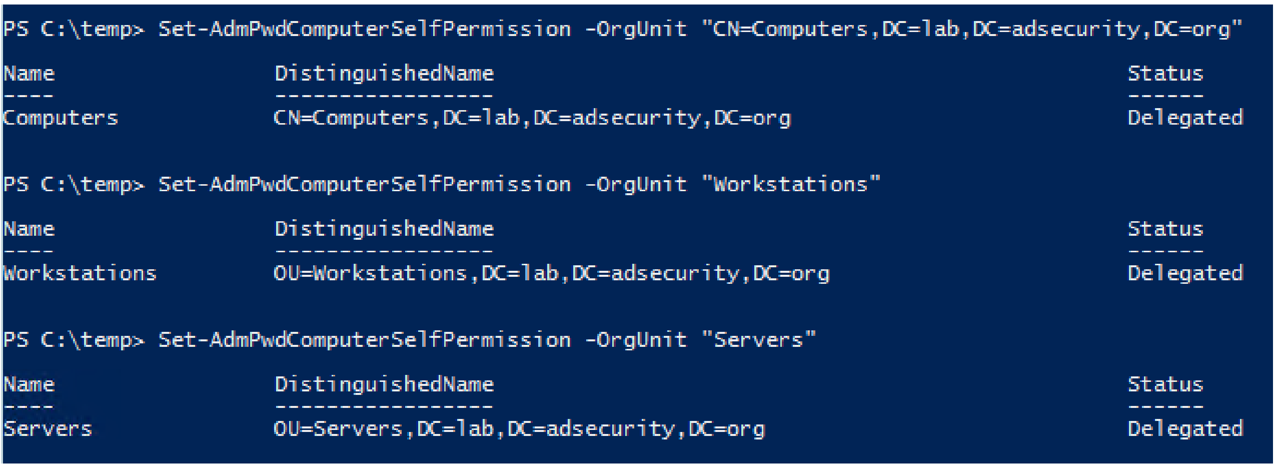
Password length
Minimum: 8 characters
Maximum: 64 characters
Default: 14 characters

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

Delegating Access to Computer Local Administrator Account Passwords

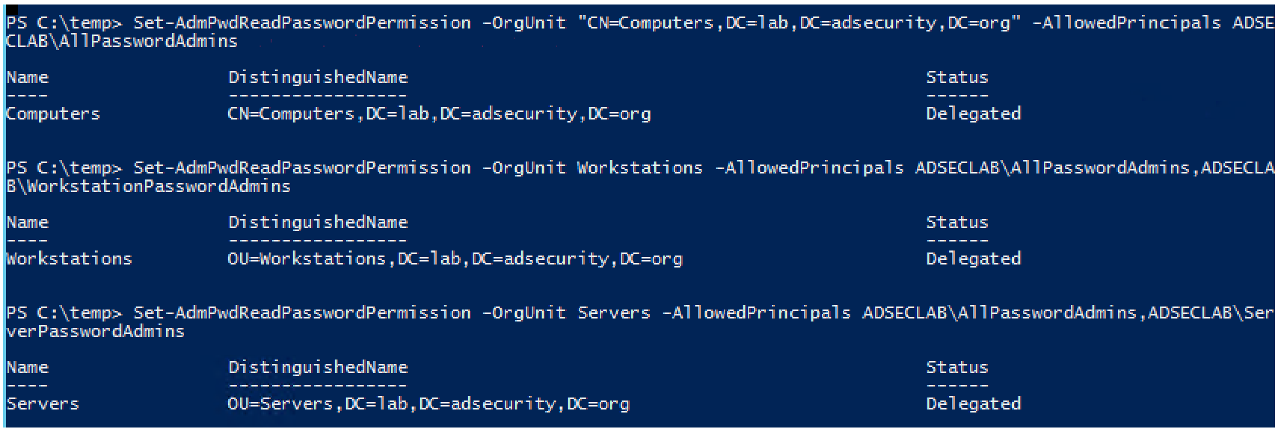
Before running any of the LAPS PowerShell cmdlets, ensure the LAPS PowerShell module is installed and imported (“Import-Module AdmPwd.PS”).

Run the included PowerShell cmdlet “*Set-AdmPwdComputerSelfPermission*” to delegate rights for every computer in an OU (or the domain) to update its own computer attribute containing the local admin password (ms-Mcs-AdmPwd).



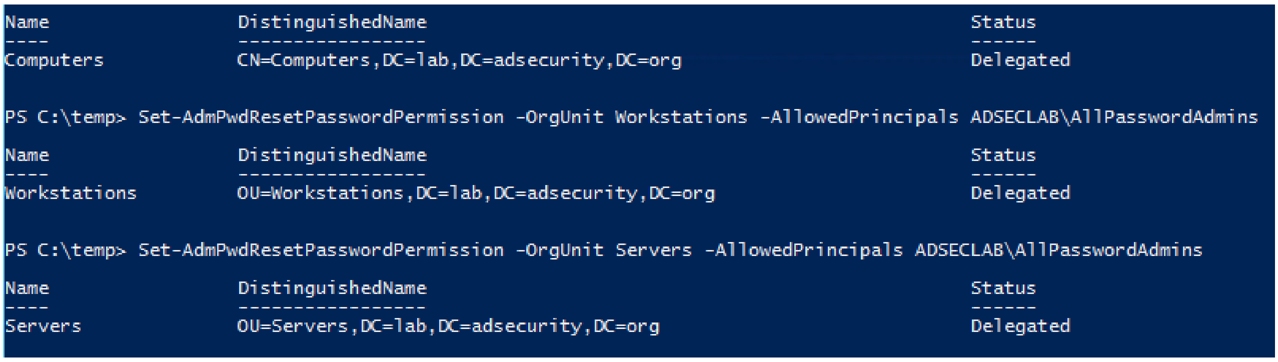
```
PS C:\temp> Set-AdmPwdComputerSelfPermission -OrgUnit "CN=Computers,DC=lab,DC=adsecurity,DC=org"

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Computers            CN=Computers,DC=lab,DC=adsecurity,DC=org                           Delegated


PS C:\temp> Set-AdmPwdComputerSelfPermission -OrgUnit "Workstations"

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Workstations         OU=Workstations,DC=lab,DC=adsecurity,DC=org                        Delegated


PS C:\temp> Set-AdmPwdComputerSelfPermission -OrgUnit "Servers"

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Servers              OU=Servers,DC=lab,DC=adsecurity,DC=org                             Delegated
```

Run the included PowerShell cmdlet "*Set-AdmPwdReadPasswordPermission*" to delegate rights for a group to view local administrator account passwords in the specified OU.



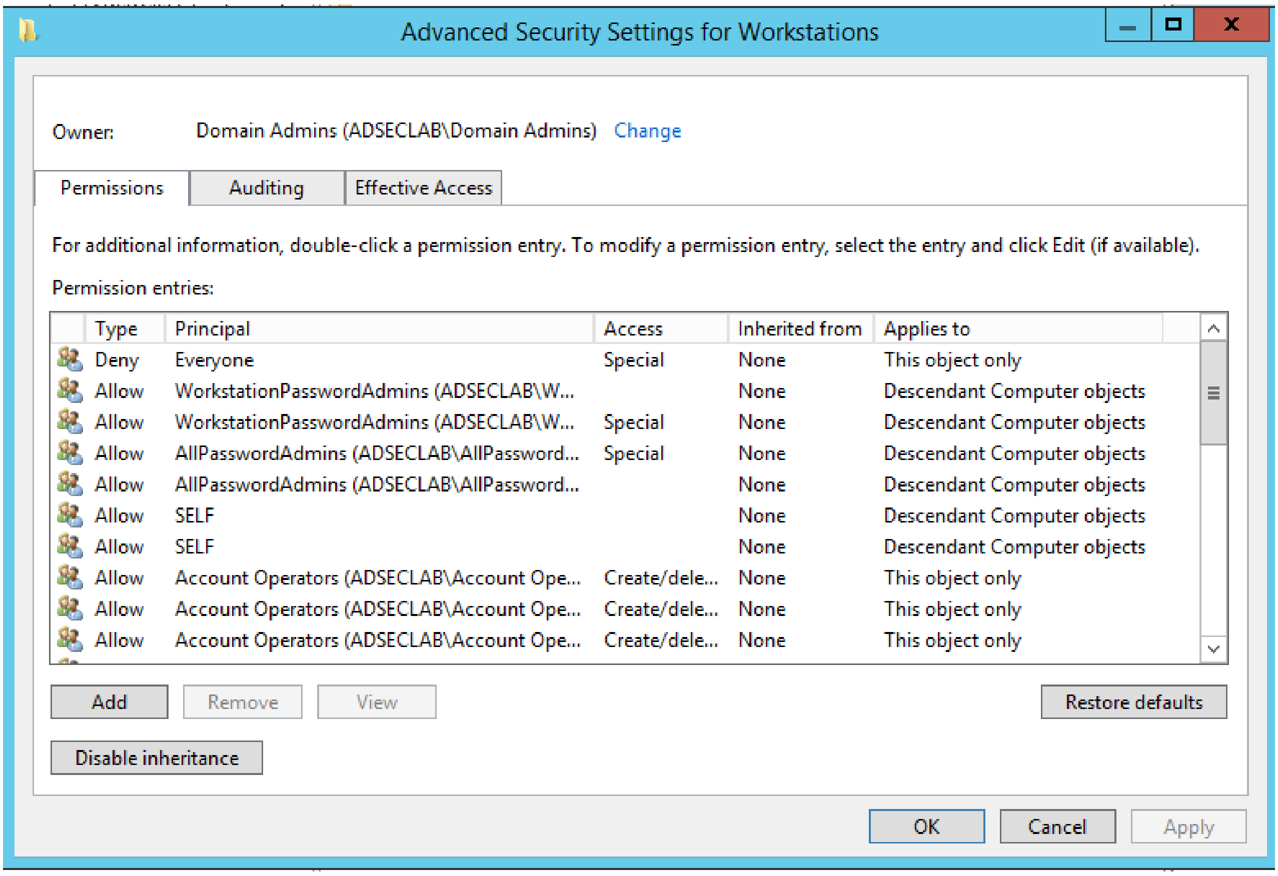
```
PS C:\temp> Set-AdmPwdReadPasswordPermission -OrgUnit "CN=Computers,DC=lab,DC=adsecurity,DC=org" -AllowedPrincipals ADSE
CLAB\AllPasswordAdmins

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Computers            CN=Computers,DC=lab,DC=adsecurity,DC=org                           Delegated


PS C:\temp> Set-AdmPwdReadPasswordPermission -OrgUnit Workstations -AllowedPrincipals ADSECLAB\AllPasswordAdmins,ADSECLA
B\WorkstationPasswordAdmins

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Workstations         OU=Workstations,DC=lab,DC=adsecurity,DC=org                        Delegated


PS C:\temp> Set-AdmPwdReadPasswordPermission -OrgUnit Servers -AllowedPrincipals ADSECLAB\AllPasswordAdmins,ADSECLAB\Ser
verPasswordAdmins

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Servers              OU=Servers,DC=lab,DC=adsecurity,DC=org                             Delegated
```

Run the included PowerShell cmdlet "*Set-AdmPwdResetPasswordPermission*" to delegate rights for a group to force local administrator account passwords in the specified OU to change (ms-Mcs-AdmPwdExpirationTime).



```
Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Computers            CN=Computers,DC=lab,DC=adsecurity,DC=org                           Delegated


PS C:\temp> Set-AdmPwdResetPasswordPermission -OrgUnit Workstations -AllowedPrincipals ADSECLAB\AllPasswordAdmins

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Workstations         OU=Workstations,DC=lab,DC=adsecurity,DC=org                        Delegated


PS C:\temp> Set-AdmPwdResetPasswordPermission -OrgUnit Servers -AllowedPrincipals ADSECLAB\AllPasswordAdmins

Name                 DistinguishedName                                                  Status
----                 -----------------                                                  ------
Servers              OU=Servers,DC=lab,DC=adsecurity,DC=org                             Delegated
```

Permissions on a Workstation OU after delegating access.



Owner: Domain Admins (ADSECLAB\Domain Admins)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	WorkstationPasswordAdmins (ADSECLAB\W...		None	Descendant Computer objects
Allow	WorkstationPasswordAdmins (ADSECLAB\W...	Special	None	Descendant Computer objects
Allow	AllPasswordAdmins (ADSECLAB\AllPassword...	Special	None	Descendant Computer objects
Allow	AllPasswordAdmins (ADSECLAB\AllPassword...		None	Descendant Computer objects
Allow	SELF		None	Descendant Computer objects
Allow	SELF		None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Account Ope...	Create/dele...	None	This object only
Allow	Account Operators (ADSECLAB\Account Ope...	Create/dele...	None	This object only
Allow	Account Operators (ADSECLAB\Account Ope...	Create/dele...	None	This object only

NOTE:
The LAPS computer attributes are flagged as “confidential” which means that Authenticated Users don’t have read access like other objects in Active Directory. Domain Admins do have read access to confidential attributes, so if this is not desirable, these “extended rights” need to be removed. Instructions on how to do this are in the LAPS Operation Guide:

> 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> | Format-Table

References & Resources:

- Microsoft Local Administrator Password Solution (LAPS)
- Microsoft Security Advisory 3062591 includes additional information on LAPS
- LAPS and permission to join computer to domain
- Local Administrator Password Solution (LAPS) Implementation Hints and Security Nerd Commentary (including mini threat model)

(Visited 127,823 times, 14 visits today)