LAPS_OperationsGuide

Local Administrator Password Management

Detailed Technical Specification

Published: June 2015

Authors:

Tom Ausburne, Microsoft

Jiri Formacek, Microsoft

Abstract: This document summarizes fundamental Operational procedures for Local Administrator Password Solution (LAPS)

Table of Contents

1 Installation

There are two parts to the installation, the management computers and the clients you want to manage.

The installation of binaries and related files is handled by the MSI package. This will install the following:

GPO CSE: must be present on each managed machine

Management tools:

- Fat client UI
- PowerShell module AdmPwd.PS
- Group Policy Editor admin templates

The default is to install the CSE only. The management tools are installed on demand.

File Reference

The installation for the Fat client UI is done to folder:

%ProgramFiles%\LAPS

AdmPwd.UI.exe
AdmPwd.Utils.config
AdmPwd.Utils.dll

The installation for the PowerShell modules is done to folder:

%WINDIR%\System32\WindowsPowerShell\v1.0\Modules\AdmPwd.PS

AdmPwd.PS.dll
AdmPwd.PS.format.ps1xml
AdmPwd.PS.psd1
AdmPwd.Utils.config
AdmPwd.Utils.dll

%WINDIR%\System32\WindowsPowerShell\v1.0\Modules\AdmPwd.PS\en-us

AdmPwd.PS.dll-Help.xml

The installation for the CSE is done to folder:

%ProgramFiles%\LAPS\CSE

AdmPwd.dll

The installation for the Group Policy files is done to folders:

%WINDIR%\PolicyDefinitions

AdmPwd.admx

%WINDIR%\PolicyDefinitions\en-US

AdmPwd.adml

1.1 Management Computers

Double click on the appropriate MSI installer for your platform (LAPS.<platform>.msi) to get started.

Click **Next**. Accept license agreement and click **Next**

For the first management machine, you should enable all the installation choices for management tools

Click **Next**.

Click **Install**.

Click **Finish**.

1.2 Managed Clients

This installation uses the same install files, AdmPwd.Setup.x64.msi and AdmPwd.Setup.x86.msi as on the management computers. These can be installed/updated/uninstalled on clients using a variety of methods including the Software Installation feature of Group Policy, SCCM, login script, manual install, etc.

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.

Example: msiexec /i \\server\share\LAPS.x64.msi /quiet

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

Note: If you install by just registering the dll it will not show up in Program and Features as shown below.

Once this is installed you can see it in Programs and Features.

1.2.1 Writable domain controller access required

Managed clients must have access to a writable domain controller in order to update the password. One way to confirm such access exists is by running the nltest.exe utility on the managed client as follows:

```
nltest.exe /dsgetdc: /writable /force
```

On success the utility will output the details of the specific domain controller that was found.

The Get-ADDomainController cmdlet may also be used for this purpose using the following syntax:

```
Get-ADDomainController -Discover -Writable -ForceDiscover
```

2 AD Preparation

2.1 Modifying the Schema

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 this command:

```
Import-module AdmPwd.PS
```

You update the Schema with this command:

```
Update-AdmPwdADSchema
```

***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.

***Note*:** Managed clients cannot update the ms-Mcs-AdmPwd attribute on an RODC, even once the above steps are performed. Managed clients must always have access to a writable domain

controller in order to update the password. See section 1.2.1.

2.2 Permissions

The Active Directory infrastructure offers advanced tools for implementation of the security model for this solution by allowing for per-attribute Access Lists (ACLs) and implementing confidential attributes for password storage. There are four sets of rights that need to be modified.

2.2.1 Removing 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.

Open **ADSIEdit**

Right Click on the OU that contains the computer accounts that you are installing this solution on and select **Properties**.

Click the **Security** tab

Click **Advanced**

Select the Group(s) or User(s) that you don’t want to be able to read the password and then click **Edit**.

Uncheck **All extended rights**

Important: This will remove ALL extended rights, not only CONTROL_ACCESS right, so be sure that all roles will retain all necessary permissions required for their regular work.

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
```

2.2.2 Adding Machine Rights

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 that are in scope of the solution and are not subcontainers of already processed containers.

2.2.3 Adding User Rights

Add the CONTROL_ACCESS permission (extended right) on ms-Mcs-AdmPwd attribute of the computer accounts to group(s) or user(s) that will be allowed to read the stored password of the managed local Administrator account on managed computers.

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

Use the same –OrgUnit name(s) as in the previous command.

Note: You can use multiple groups and users in the same command separated by comma.

Example:

```
Set-AdmPwdReadPasswordPermission -OrgUnit Servers -AllowedPrincipals
contoso\Administrator,contoso\HelpDesk,contoso\PwdAdmins
```

Add the Write permission on ms-Mcs-AdmPwdExpirationTime attribute of computer accounts to group(s) or user(s) that will be allowed to force password resets for the managed local Administrator account on managed computers.

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

Use the same –OrgUnit name(s) as in the previous commands.

Note: You can use multiple groups and users in the same command separated by comma.

Example:

Set-AdmPwdResetPasswordPermission -OrgUnit Servers -AllowedPrincipals contoso\Administrator,contoso\HelpDesk,contoso\PwdAdmins

2.2.4 Security implications of domain-join-by-privilege

Active Directory by default allows ordinary users to join machines to the domain, up to the limit imposed by the msDS-MachineAccountQuota attribute. The user must have local Administrator privileges on a machine in order to perform the join. When a machine is joined this way, the resultant security configuration on the machine account allows the joining user to read the value of the ms-Mcs-AdmPwd attribute, even after the user in question no longer has local Administrator privileges on a machine.

Machine that have been joined this way can be discovered by querying the msDS-CreatorSid attribute attribute, for example:

```
Get-ADComputer -LdapFilter '(msds-CreatorSid=*)' -SearchBase '<domain-or-OU-DN>' -SearchScope Subtree
```

You can prevent this issue by disabling the ability of ordinary users to join machines to the domain. This can be done by setting the ms-DS-MachineAccountQuota attribute to zero.

Additional background context can be found in the following topics:

Default limit to number of workstations a user can join to the domain

MS-DS-Creator-SID attribute

MS-DS-Machine-Account-Quota attribute

*Microsoft would like to thank **Metin Yunus Kandemir** for finding this issue.*

3 Group Policy

3.1 Changing the Group Policy Settings

The settings are located under Computer Configuration\Administrative Templates\LAPS.

3.2 Enabling the local administrator password management

Management of password of local administrator account must be enabled so as the CSE can start managing it:

3.3 Password parameters

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.

3.3.1 Administrator account name

If you have decided to manage custom local Administrator account, you must specify its name in Group Policy.

Note: DO NOT configure when you use the built-in admin account, even if you renamed it. That account is auto-detected by well-known SID. DO configure when you use a custom local admin account.

3.4 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:

4 Managing Clients

4.1 Viewing password settings

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. The Expiration date is stored as the number of 100-nanosecond intervals that have elapsed since the 0 hour on January 1, 1601 untill the date/time that is being stored. The time is always stored in Greenwich Mean Time (GMT) in the Active

Directory. If you want to manually convert it use this command:

```
w32tm /ntte <number you want to convert>
```

There is also a graphical interface available. When you install the program on a computer where you want the ability to easily retrieve the password just select the Fat client UI option.

The program you want to run is **C:\Program Files\LAPS\AdmPwd.UI.exe**. It will be in the menu and looks like this:

Or this on Windows 7.

Launch the interface, enter the client name and click **Search**.

You can also get the password using PowerShell.

```
Get-AdmPwdPassword -ComputerName <computername>
```

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.

If they have installed the RSAT tools and run Active Directory Users and Computers (ADUC) to view the password it will show as <not set>.

This information is not seen because the extended rights were removed and only certain individuals and groups were granted the rights to see this.

4.2 Resetting the password

To manually reset the password, just click the Set button in LAPS UI tool. When a Group Policy refresh runs, password will be reset.

You can also plan password expiration for the future. To do so, enter desired expiration date/time into respective field.

You can also reset the password using PowerShell.

```
Reset-AdmPwdPassword -ComputerName <computername> -WhenEffective <date time>
```

5 Troubleshooting

This solution has a variety of logging options for troubleshooting purposes.

5.1 Event Logging and Auditing

5.1.1 Client Logging

The CSE logs all events in the Application Event Log of local computer. Log messages are English only, but can be localized or additional language can be added, if necessary.

The amount of events that are logged is configurable via the following registry REG_DWORD value:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}\ExtensionDebugLevel

This value is not there by default and must be added.

Possible values are as follows:

Value	Meaning
0	Silent mode; log errors only When no error occurs, no information is logged about CSE activity This is a default value
1	Log Errors and warnings
2	Verbose mode, log everything

5.1.2 Event IDs

The Event source for all events reported by CSE is always “AdmPwd”. The following table summarizes the events that can occur in the Event Log:

ID	Severity	Description	Comment
2	Error	Could not get computer object from AD. Error %1	This event is logged in case that CSE is not able to connect to computer account for local computer in AD. %1 is a placeholder for error code returned by function that retrieves local computer name, converts it to DN and connects to object, specified by the DN
3	Error	Could not get local Administrator account. Error %1	This event is logged in case that CSE is not able to connect to managed local Administrator account. %1 is a placeholder to error code returned by function that detects the name of local administrator’s account and connects to the account

ID	Severity	Description	Comment
4	Error	Could not get password expiration timestamp from computer account in AD. Error %1.	This event is logged in case that CSE is not able to read the value of ms-Mcs-AdmPwdExpirationTime of computer account in AD %1 is a placeholder for error code returned by function that reads the value of the attribute and converts the value to unsigned __int64 type
5	Error	Validation failed for new local admin password against local password policy. Error %1.	This event is logged when password validation against local password policy fails.
5	Information	Validation passed for new local admin password.	This event is logged when password is successfully validated against local password policy
6	Error	Could not reset local Administrator's password. Error %1	This event is logged in case that CSE is not able to reset the password of managed local Administrator account. %1 is a placeholder for error returned by NetUserSetInfo() API
7	Error	Could not write changed password to AD. Error %1.	This event is logged in case that CSE is not able to report new password and timestamp to AD. %1 is a placeholder for error code returned by ldap_mod_s call
10	Warning	Password expiration too long for computer (%1 days). Resetting password now.	This event is logged in case that CSE detects that password expiration for computer is longer than allowed by policy in place while protection against excessive password age is turned on

ID	Severity	Description	Comment
11	Information	It is not necessary to change password yet. Days to change: %1.	This event is logged after CSE detects that it is not yet the time to reset the password %1 is a placeholder for number of 24-hour's intervals that remain till the password will be reset
12	Information	Local Administrator's password has been changed.	This event is logged after CSE resets the password of managed local Administrator account
13	Information	Local Administrator's password has been reported to AD.	This event is logged after CSE reports the password and timestamp to AD
14	Information	Finished successfully	This event is logged after CSE performed all required tasks and is about to finish
15	Information	Beginning processing	This event is logged when CSE starts processing
16	Information	Admin account management not enabled, exiting	This event is logged when admin account management is not enabled

Note: Generally, all events with severity "Error" are blocking. When any error occurs, no other tasks are performed and CSE terminates processing.

5.2 Problem Scenarios

Symptom: Client gets Event ID 7, "Could not write changed password to AD. Error 0x80070032" in the Event log.

Solution: The client is not in a managed OU. Move it to a managed OU or run the PowerShell commands to add the Machine Rights to the OU the client is in.

Symptom: When importing AdmPwd.PS module, you get error “Import-Module: Could not load file or assembly 'file:///C:\Windows\system32\WindowsPowerShell\v1.0\Modules\admpwd.ps\AdmPwd.PS.dll' or one of its dependencies. This assembly is built by a runtime newer than the currently loaded runtime and cannot be loaded.”

Solution: You need to allow PowerShell to load .NET Framework 4. To allow this, you need to change powershell.exe.config to contain this:

```
<?xml version="1.0"?>
<configuration>
   <startup useLegacyV2RuntimeActivationPolicy="true">
      <supportedRuntime version="v4.0.30319"/>
      <supportedRuntime version="v2.0.50727"/>
   </startup>
</configuration>
```

Symptom: Everything is installed but the password isn’t updating on the client and nothing is logged in the Event Log.

Solution: The CSE hasn’t been enabled with a Group Policy that applies to the client. Set the policy “Enable local admin password management” to Enabled

Symptom: Everything is installed but the password isn’t getting updated in Active Directory

Solution: The client does not have network connectivity to a writable domain controller. Ensure that the client is able to see a writable domain controller. See section 1.2.1.

Symptom: After running the Schema update, the new attributes aren’t showing in the computer properties.

Solution: If the status of the Schema update was successful you may be experiencing replication issues or latency. In larger environments this attribute population may take some time to propagate.

Symptom: Users that haven’t been specifically granted permissions can still see the password.

Solution: This is usually due to not removing the “All Extended rights” permission from groups and users. Check the effective rights on the computer in question.

5.3 Auditing

Auditing users who successfully query and read the local administrator password for a computer can be accomplished by using a PowerShell cmdlet. You may need to run Import-module AdmPwd.PS if this is a new window.

> 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 a password is successfully read, a 4662 event is logged in the Security log of the Domain Controller.

You will notice that the schemaIDGUID is reflected in the Event properties.

Revision #1
Created 22 December 2023 02:11:42 by ColtM
Updated 7 August 2024 23:24:38 by ColtM