Operations Guide

Management of password of local Administrator account



Version 1.0

Prepared by

Tom Ausburne  
Jiri Formacek

Table of Contents

[1 Installation 1](#_Toc388979091)

[1.1 Management Computers 2](#_Toc388979092)

[1.2 Managed Clients 4](#_Toc388979093)

[2 AD Preparation 5](#_Toc388979094)

[2.1 Modifying the Schema 5](#_Toc388979095)

[2.2 Permissions 6](#_Toc388979096)

[2.2.1 Removing Extended Rights 6](#_Toc388979097)

[2.2.2 Adding Machine Rights 7](#_Toc388979098)

[2.2.3 Adding User Rights 7](#_Toc388979099)

[3 Group Policy 9](#_Toc388979100)

[3.1 Registration of CSE with chosen Group Policy Object 9](#_Toc388979101)

[3.2 Changing the Group Policy Settings 10](#_Toc388979102)

[4 Managing Clients 12](#_Toc388979103)

[4.1 Viewing password settings 12](#_Toc388979104)

[4.2 Changing password settings 15](#_Toc388979105)

[5 Troubleshooting 16](#_Toc388979106)

[5.1 Event Logging and Auditing 16](#_Toc388979107)

[5.1.1 Client Logging 16](#_Toc388979108)

[5.1.2 Event IDs 16](#_Toc388979109)

[5.2 Problem Scenarios 18](#_Toc388979110)

[5.3 Auditing 19](#_Toc388979111)

[5.3.1 Using Audit Collection Services (ACS) to gather events 21](#_Toc388979112)

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%\AdmPwd

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

The installation for the CSE is done to folder:

%ProgramFiles%\AdmPwd\CSE

AdmPwd.dll

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

%WINDIR%\PolicyDefinitions

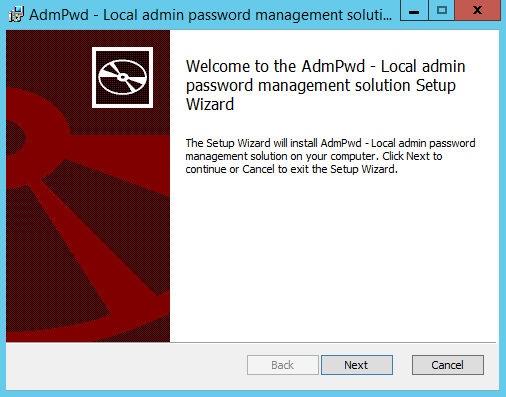
AdmPwd.admx

%WINDIR%\PolicyDefinitions\en-US

AdmPwd.adml

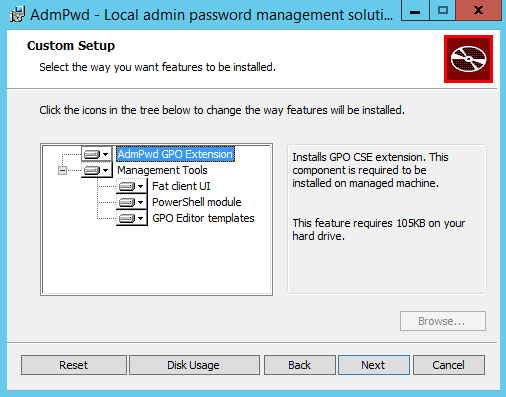
* 1. Management Computers

Extract the files from the Installers.zip to a folder. There will be two files, AdmPwd.Setup.x64.msi and AdmPwd.Setup.x86.msi. Copy these files to a working directory. Double click on the appropriate file to get started.

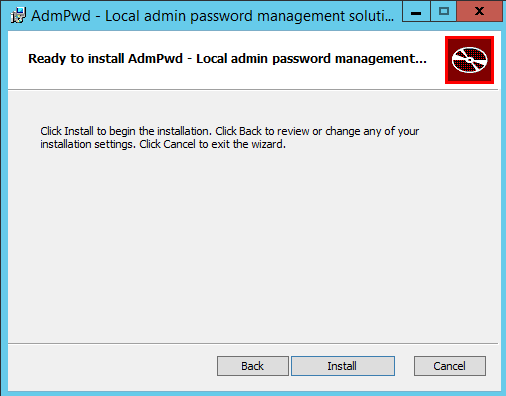


Click **Next.**

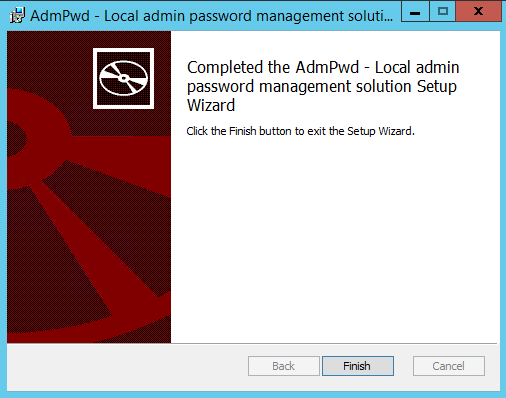
For the first machine you should enable all the installation choices.



Click **Next**.



Click **Install**.



Click **Finish**.

* 1. 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>\AdmPwd.Setup.x64.msi /quiet or

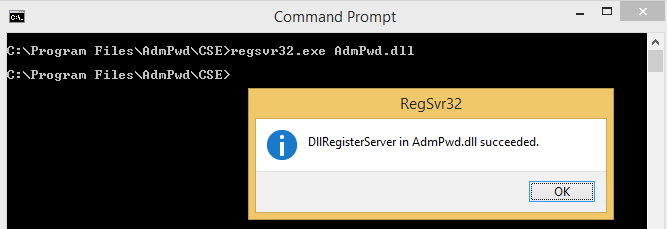
msiexec /i <file location>\AdmPwd.Setup.x86.msi

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

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

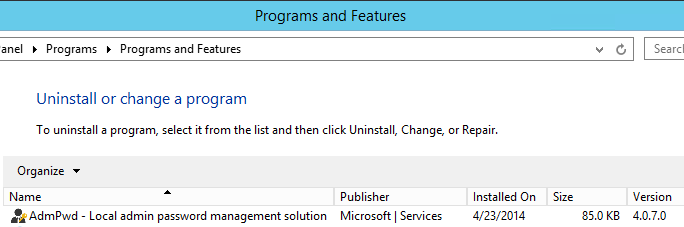
Or you copy the AdmPwd.dll to the target computer and use this command:

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. AD Preparation
   1. Modifying the Schema

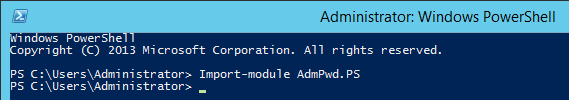
The Active Directory Schema needs to be extended by two new attributes that store the password of the built-in Administrator account for each computer and the timestamp of password expiration. Both attributes are added to the may-contain attribute set of the computer class.

ms-MCS-AdmPwd – Stores the password in clear text

ms-MCS-AdmPwdExpirationTime – Stores the time to reset the password

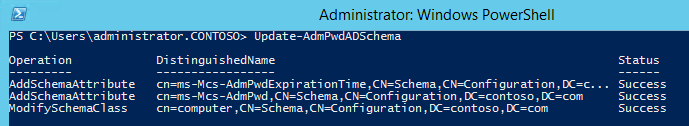
To update the Schema you first need to import the PowerShell module. Open up an Administrative PowerShell window and use this command:

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 the RODC Filtered Attribute Set, please refer to <http://technet.microsoft.com/en-us/library/cc754794(v=WS.10).aspx>.

* 1. Permissions

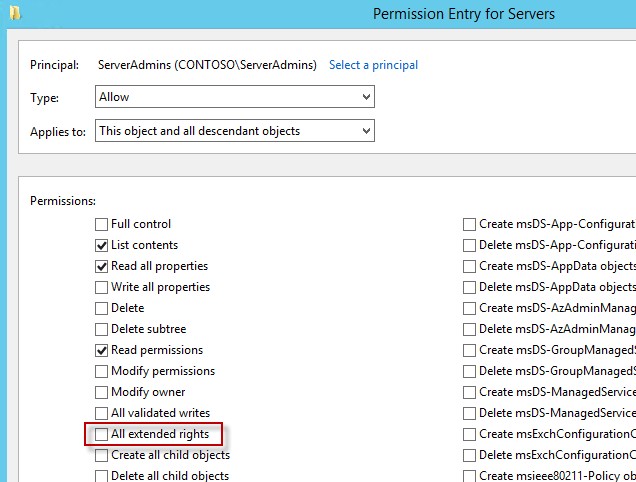
The Active Directory infrastructure offers advanced tools for implementation of the security model for this solution by allowing for per-attribute Access Lists (ACLs) and implementing confidential attributes for password storage. There are four sets of rights that need to be modified.

* + 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.

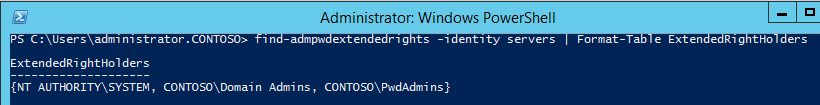
1. Open **ADSIEdit**
2. **Right Click on the** OU that contains the computer accounts that you are installing this solution on and select **Properties**.
3. Click the **Security** tab
4. Click **Advanced**
5. Select the Group(s) or User(s) that you don’t want to be able to read the password and then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



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.

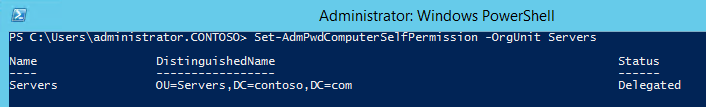
Find-AdmPwdExtendedrights -identity :<OU name> | Format-Table ExtendedRightHolders



* + 1. 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 built-in 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>



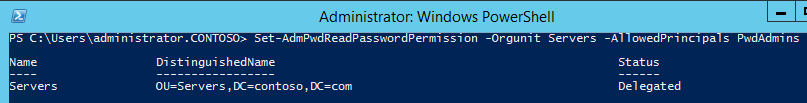
Repeat this procedure for any additional OUs that contain computer accounts that are in scope of the solution and are not subcontainers of already processed containers.

* + 1. 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 built-in 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.



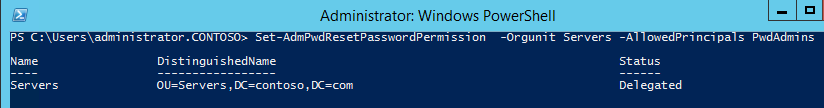
Note: You can use multiple groups and users in the same command separated by comma.

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 built-in 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.

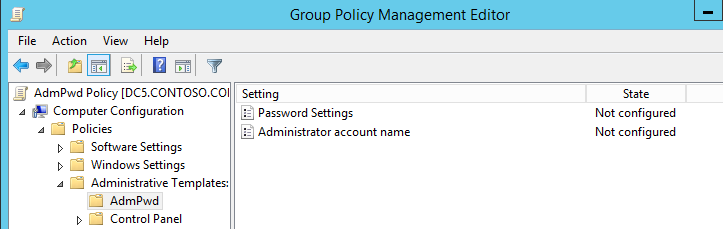


Note: You can use multiple groups and users in the same command separated by comma.

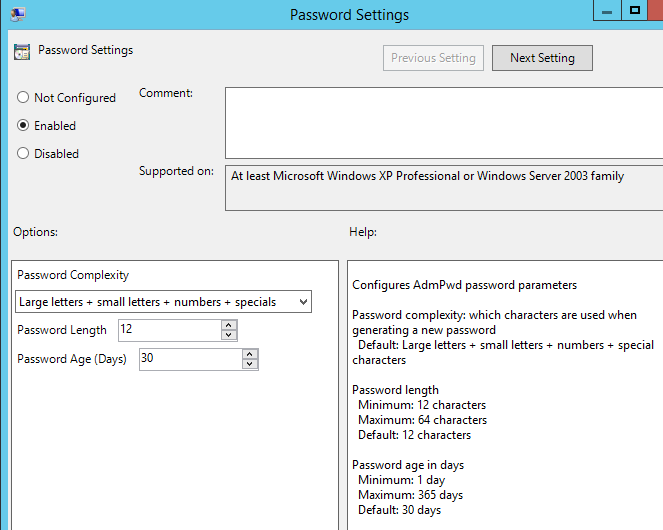
Example:   
  
Set-AdmPwdResetPasswordPermission -OrgUnit Servers -AllowedPrincipals contoso\Administrator,contoso\HelpDesk,contoso\PwdAdmins

1. Group Policy
   1. Changing the Group Policy Settings

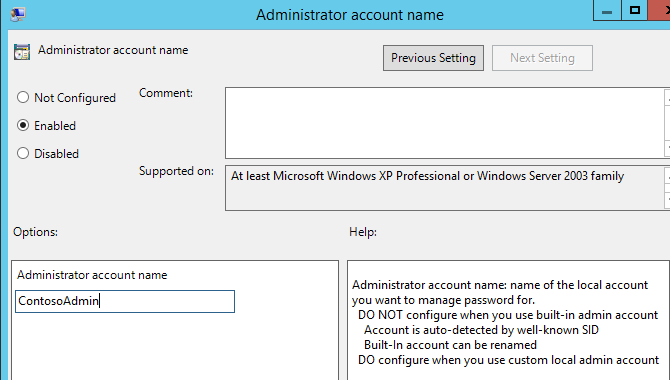
By default this solution uses a password with password complexity, 12 characters and changes the password every 30 days. You can change the values to suit your needs by editing a Group Policy. The settings are located in under Computer Configuration\Administrative Templates\AdmPwd.



You can change the individual password settings to fits your needs.



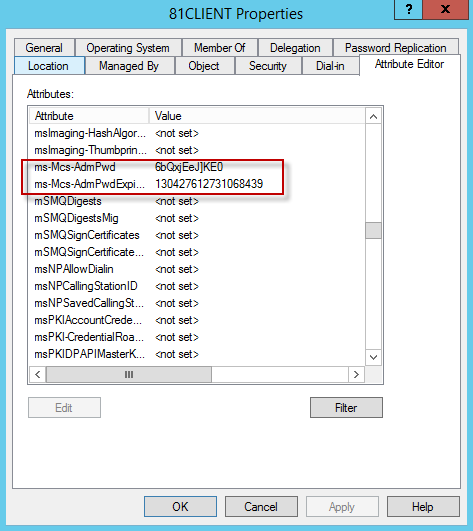
If you have renamed or disabled the local Administrator account and created a separate account, you can specify this in Group Policy.



**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.

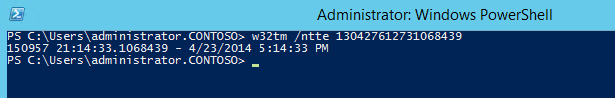
1. Managing Clients
   1. Viewing password settings

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.

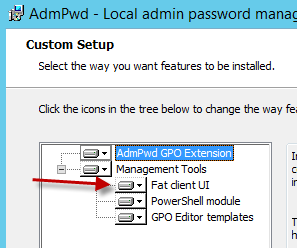


The password is stored in plain text. The Expiration date is stored as the number of 100-nanosecond intervals that have elapsed since the 0 hour on January 1, 1601 untill the date/time that is being stored. The time is always stored in Greenwich Mean Time (GMT) in the Active Directory. If you want to manually convert it use this command:

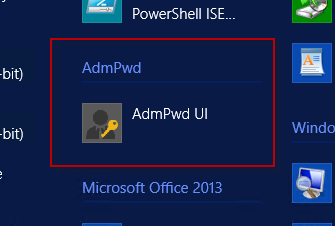
w32tm /ntte <number you want to convert>



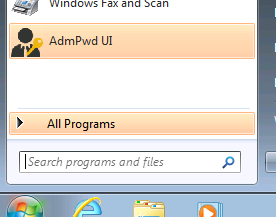
There is also a graphical interface available. When you install the program on a computer where you want the ability to easily retrieve the password just select the Fat client UI option.



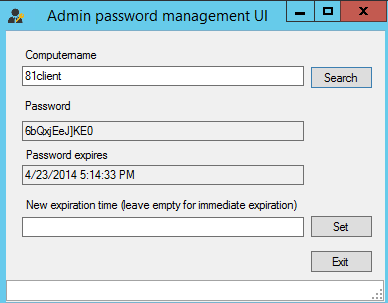
The program you want to run is **C:\Program Files\AdmPwd\ AdmPwd.UI.exe**. It will be in the menu and looks like this:



Or this on Windows 7.

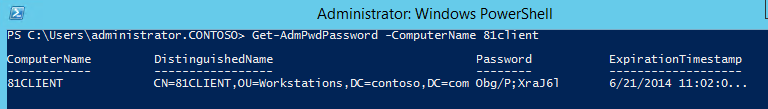


Launch the interface, enter the client name and click **Search**.

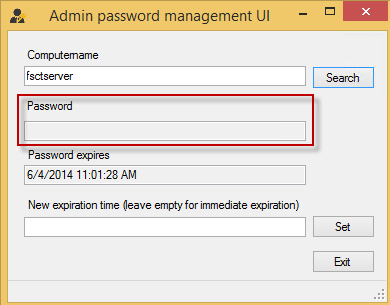


You can also get the password using PowerShell.

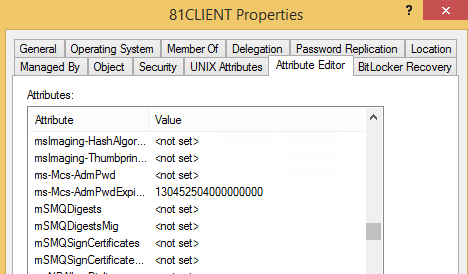
Get-AdmPwdPassword -ComputerName <computername>



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.



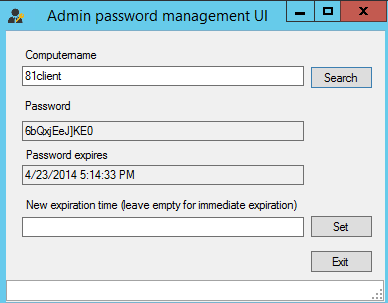
If they have installed the RSAT tools and run Active Directory Users and Computers (ADUC) to view the password it will show as <not set>.



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

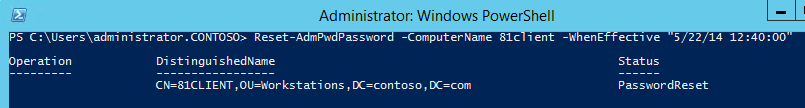
* 1. Changing password settings

To manually reset the password click the Set button. When a Group Policy refresh runs it will be updated.



You can also reset the password using PowerShell.

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



1. Troubleshooting

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

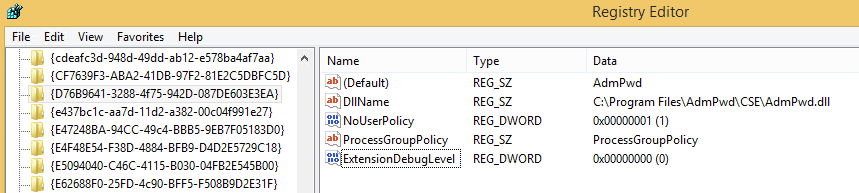
* 1. Event Logging and Auditing
     1. Client Logging

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 |

* + 1. 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 |
| --- | --- | --- | --- |
| 1 | Error | Could not initialize COM. Error %1 | This event is logged in case that CSE fails to initialize COM layer (which is required for ADSI to work)  %1 is a placeholder for error code returned by the call of CoInitializeEx() |
| 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 built-in Administrator account.  %1 is a placeholder to error code returned by function that detects the name of local administrator’s account, creates connection string for WinNT: ADSI provider and connects to the account |
| 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 | Warning | Could not get loglevel from registry. Error %1 | This event is logged in case that CSE is not able to read logging level from registry (such as in case that value exists, but is a different type than REG\_DWORD)  When this event occurs, CSE continues working and uses default logging level |
| 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 built-in Administrator account.  %1 is a placeholder for error returned by IADsUser::SetPassword() method |
| 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 function that converts timestamp to IADsLargeInteger and then calls IADs::Put() and IADs::SetInfo()methods |
| 8 | Warning | Could not get password length from registry, using default value. Error %1. | This event is logged in case that CSE is not able to read password length configuration value from registry (such as in case that value exists, but is a different type than REG\_DWORD)  When this event occurs, CSE continues working and uses default value |
| 9 | Warning | Could not get password complexity from registry, using default value. Error %1. | This event is logged in case that CSE is not able to read password complexity configuration value from registry (such as in case that value exists, but is a different type than REG\_DWORD)  When this event occurs, CSE continues working and uses default value |
| 10 | Warning | Could not get password age from registry, using default value. Error %1. | This event is logged in case that CSE is not able to read max password age configuration value from registry (such as in case that value exists, but is a different type than REG\_DWORD)  When this event occurs, CSE continues working and uses default value |
| 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 built-in 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 | Password length not configured in GPO or configured value is outside allowed boundaries. Will use default value. |  |
| 17 | Information | Password complexity not configured in GPO or configured value is outside allowed boundaries. Will use default value. |  |
| 18 | Information | Password age not configured in GPO or configured value is outside allowed boundaries. Will use default value. |  |
| 19 | Information | Admin account name not configured in GPO. Will manage builtin admin account. |  |

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

* 1. Problem Scenarios

**Symptom**: Client gets Event ID 7, “Could not write changed password to AD. Error 0x80070005” 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**: Client gets Event IDs 16, 17 and 18 in the Event log when logging is set to 1 or 2.

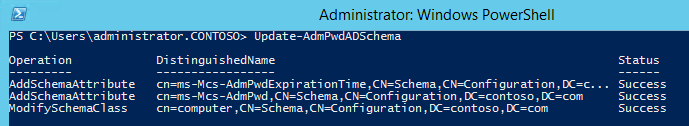
**Solution**: The client’s password has expired but there has been no specific group policy set to modify the default settings. This is not a problem if you want the default password settings.

**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. Run the PowerShell command to register AdmPwd with a Group Policy that applies to the client.

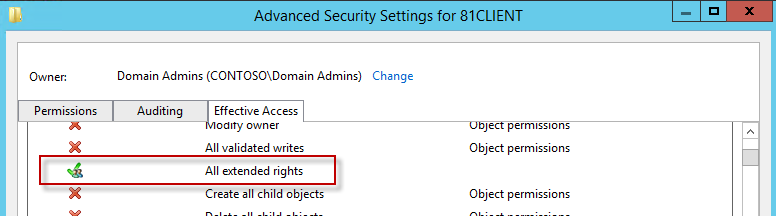
**Symptom**: After running the Schema update, the new attributes aren’t showing in the computer properties.

**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.

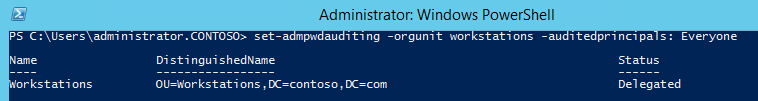
**Solution**: This is usually due to not removing the “All Extended rights” permission from groups and users. Check the effective rights on the computer in question.



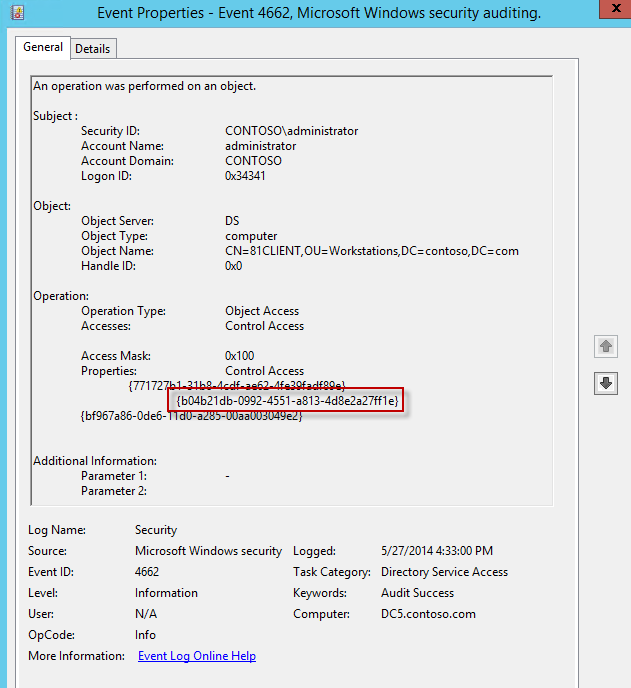
* 1. Auditing

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.

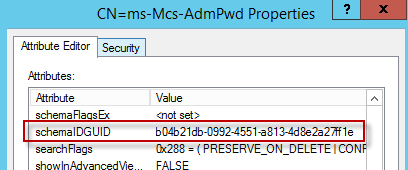
Set-AdmPwdAuditing –OrgUnit: <name of OU on which you want to setup the auditing> -AuditedPrincipals: :<identification of users/groups whose access to password shall be audited>



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.



* + 1. Using Audit Collection Services (ACS) to gather events

If you are running System Center Operation Manager and using ACS, the following steps will enable you to gather events specific to AdmPwd. This query supports both W2K3 and W2K8+ eventIDs. The procedure will be performed using adtAdmin.exe command line tool on ACS collector server.

*Note: The adtAdmin.exe tool is installed in %Systemroot%\System32\Security\AdtServer folder by default.*

This procedure consists of the following steps:

* Open an elevated command prompt on ACS collector server
* Navigate to folder %Systemroot%\System32\Security\AdtServer
* Run the following command line:
  + Adtadmin –getquery > query.txt
* Open the file query.txt in notepad
* Navigate to the end of the output line, just BEFORE the last character, which is an apostrophe
* Insert the following text at the position before the apostrophe (including the leading space):
  + Or(EventId=566 and String03 LIKE '[%][%]7688%' and String01 LIKE '[%]{bf967a86-0de6-11d0-a285-00aa003049e2}%') Or (EventId=4662 and String03 LIKE '[%][%]7688%' and String01 LIKE '[%]{bf967a86-0de6-11d0-a285-00aa003049e2}%'
* Copy the entire query string to the clipboard (including the leading and trailing apostrophe)
* Switch to a command line and enter the following command, but do NOT press Enter key after it:
  + AdtAdmin -setquery -query:
* Place the query string from clipboard to the end of command line
* Press Enter