

Implementare Local Administrator Password Solution (LAPS)

Local Administrator Password Solution (LAPS) è un software Microsoft che permette di gestire le password degli amministratori locali in Windows. Quando installate il sistema operativo vi viene chiesto di inserire la password per l'utente amministratore locale del computer e spesso utilizzate questo account e la password impostata per potervi loggare localmente alla macchina se non riuscite a loggarvi al dominio. Gestire manualmente queste password, ammesso e non concesso che non sia un'unica password per tutti i vostri computer, è un'impresa non da poco quando si devono gestire centinaia se non migliaia di macchine. Immaginate cosa potrebbe succedere se la password venisse rivelata a persone indesiderate.

Local Administrator Password Solution (LAPS) permette di creare un repository centralizzato dove conservare le password per gli amministratori locali delle macchine che sono collegate al dominio e vi permette di:

- Avere una password univoca e quindi diversa su ogni computer che LAPS gestisce
- Cambiare regolarmente la password dell'amministratore locale
- Conservare le password in un attributo del computer in Active Directory
- Configurare e controllare gli accessi alle password
- Trasmettere in maniera sicura le password ai computer gestiti

LAPS funziona sia sulle versioni a 32 bit che a 64 bit di Windows 10, Windows 8, Windows 8.1, Windows 7, Windows Vista, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 e richiede che il livello funzionale del dominio sia almeno Windows Server 2003 o successivo.

N.B: Dopo l'installazione, prima di utilizzare il tool sarà necessario, aggiornare lo schema di Active Directory con la cmdlet **Update-AdmPwdADSchema** (inclusa nel modulo PowerShell che verrà installato insieme al tool) e distribuire il client MSI (magari utilizzando le Group Policy client-side extension).

Il tool è scaricabile dall'indirizzo <https://www.microsoft.com/en-us/download/details.aspx?id=46899>

Come funziona LAPS

Dopo aver distribuito il client sulle macchine da amministrare, ogni volta che avviene il refresh delle Group Policy, vengono effettuate le seguenti operazioni:

- LAPS controlla se la password dell'amministratore è scaduta
- Se la password è scaduta allora viene generata dinamicamente una nuova password, che viene conservata in un particolare attributo di AD del computer, e viene trasmessa al computer e quindi assegnata all'account amministrativo

Installazione di LAPS

Prima di poter configurare i computer, sarà necessario spostarli in una OU dedicata, a cui verranno successivamente associate le Group Policy per la gestione.

Scaricate LAPS e installate solo i tool di gestione **sul server**. Nel mio caso l'ho installato sul domain controller. Disabilitate l'AdmPwd GPO Extension ed abilitate tutti management Tools, come mostrato in figura:



Figura 1: Schermata iniziale del tool Local Administrator Password Solution

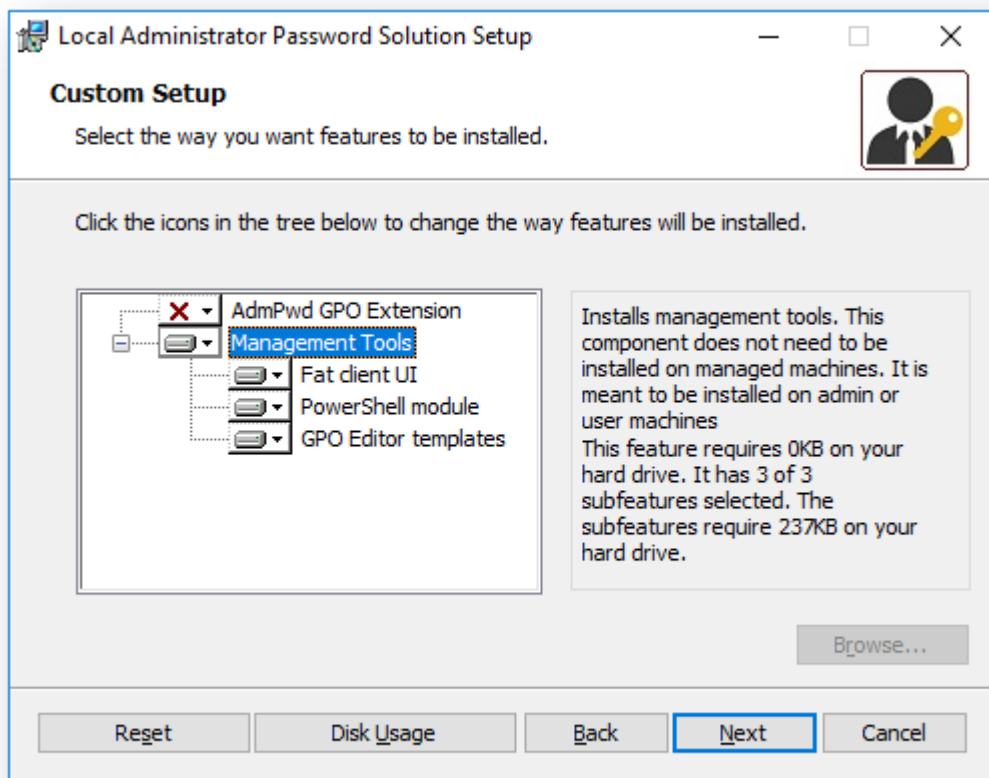


Figura 2: Configurazione dei parametri del tool

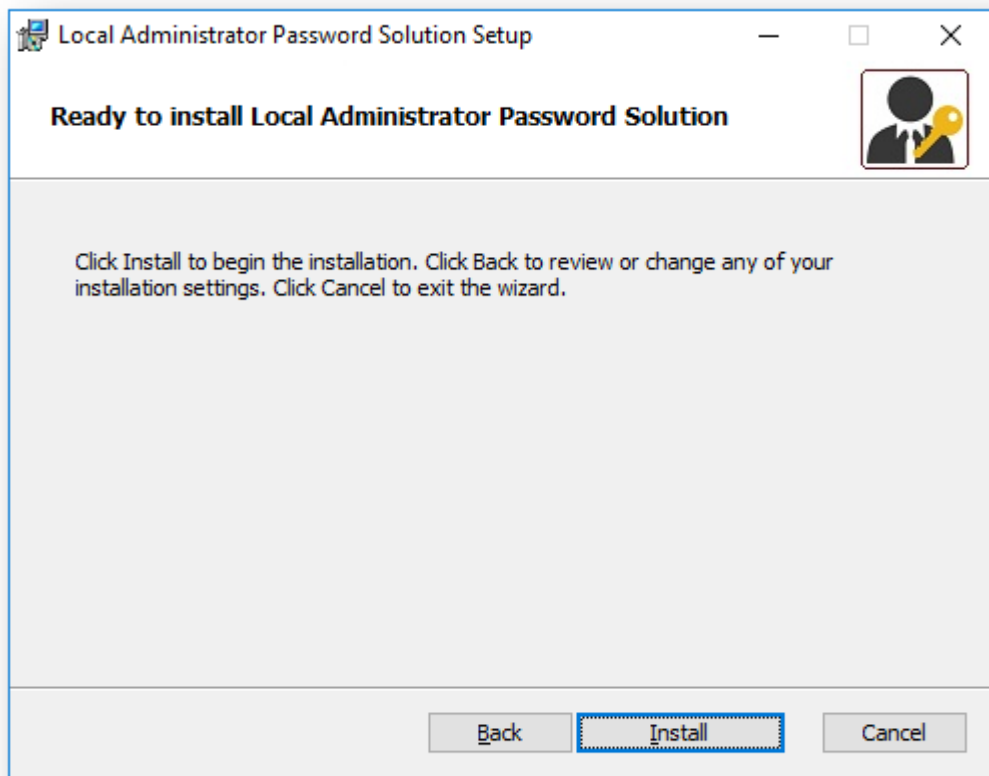


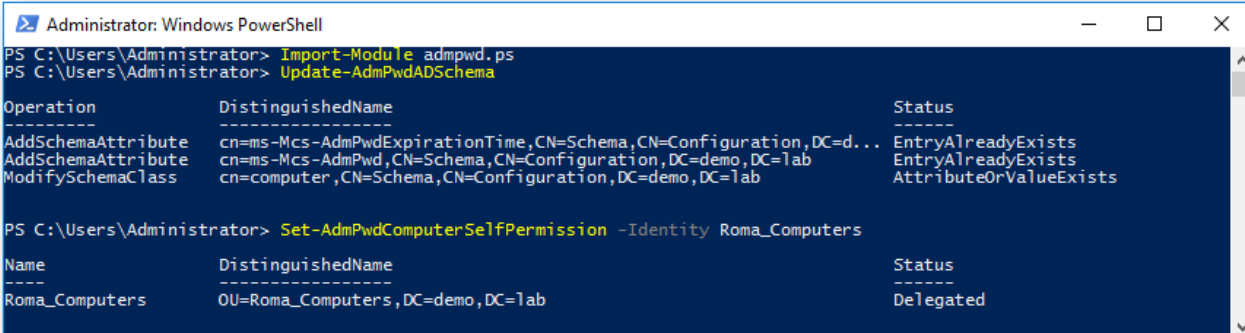
Figura 3: Completamento dell'installazione

Terminata l'installazione del tool, lanciate un prompt di PowerShell con privilegi elevati ed eseguite i seguenti comandi:

```
1 Import-Module admpwd.ps
2
3 Update-AdmPwdADSchema
4
5 Set-AdmPwdComputerSelfPermission -Identity "Roma_Computers" (Roma_Computers
   è l'organizational unit dentro la quale ci sono i computer da gestire)

Comando alternativo
6 Set-AdmPwdComputerSelfPermission -OrgUnit
   "OU=Computers,DC=domain,DC=com"
```

Ricordatevi che per poter aggiornare lo schema dovete eseguire la cmdlet **Update-AdmPwdADSchema** con privilegi di Enterprise Admin o di Schema Admin.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Import-Module admpwd.ps
PS C:\Users\Administrator> Update-AdmPwdADSchema

Operation                DistinguishedName                Status
-----
AddSchemaAttribute       cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=d... EntryAlreadyExists
AddSchemaAttribute       cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=demo,DC=lab      EntryAlreadyExists
ModifySchemaClass        cn=computer,CN=Schema,CN=Configuration,DC=demo,DC=lab          AttributeOrValueExists

PS C:\Users\Administrator> Set-AdmPwdComputerSelfPermission -Identity Roma_Computers

Name                DistinguishedName                Status
-----
Roma_Computers      OU=Roma_Computers,DC=demo,DC=lab  Delegated
```

Figura 4: Configurazione e aggiornamento dello Schema

A questo punto create una nuova GPO e collegatela alla OU che volete gestire. Io ho chiamato la GPO con il nome LAPS e l'ho collegata alla OU chiamata Roma_Computers. Editate la GPO e dopo esservi spostati nel ramo **Computer Configuration→Policies→Administrative Templates→LAPS**, modificate il parametro **Enable local admin password management** mettendolo su **Enabled** e il parametro **Password Settings** scegliendo lunghezza e durata della password, come mostrato in figura:

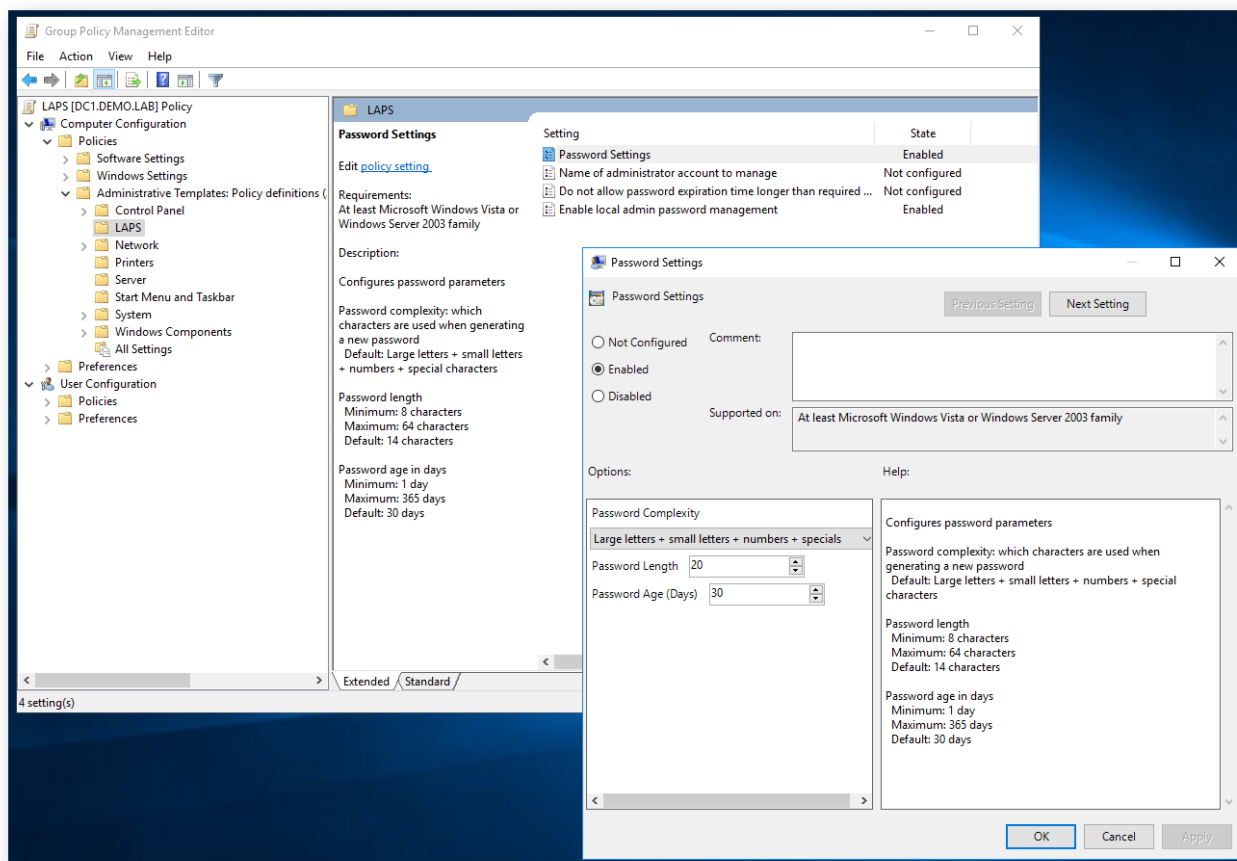


Figura 5: Configurazione dei parametri della Group Policy per il LAPS

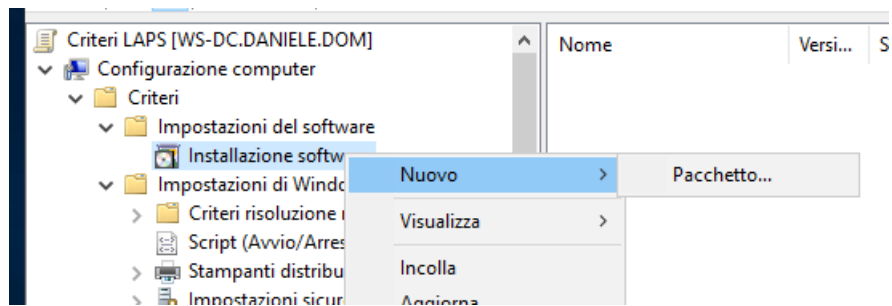
NOTA: Per impostazione predefinita LAPS cambia la password all'amministratore di built-in, anche se gli avete cambiato nome perché fa riferimento all'utente con il well-known SID che finisce per **.500**; nel caso utilizzate un utenza personalizzata allora sarà necessario configurare anche la policy **Name of administrator account to manage**.

Distribuzione del client LAPS

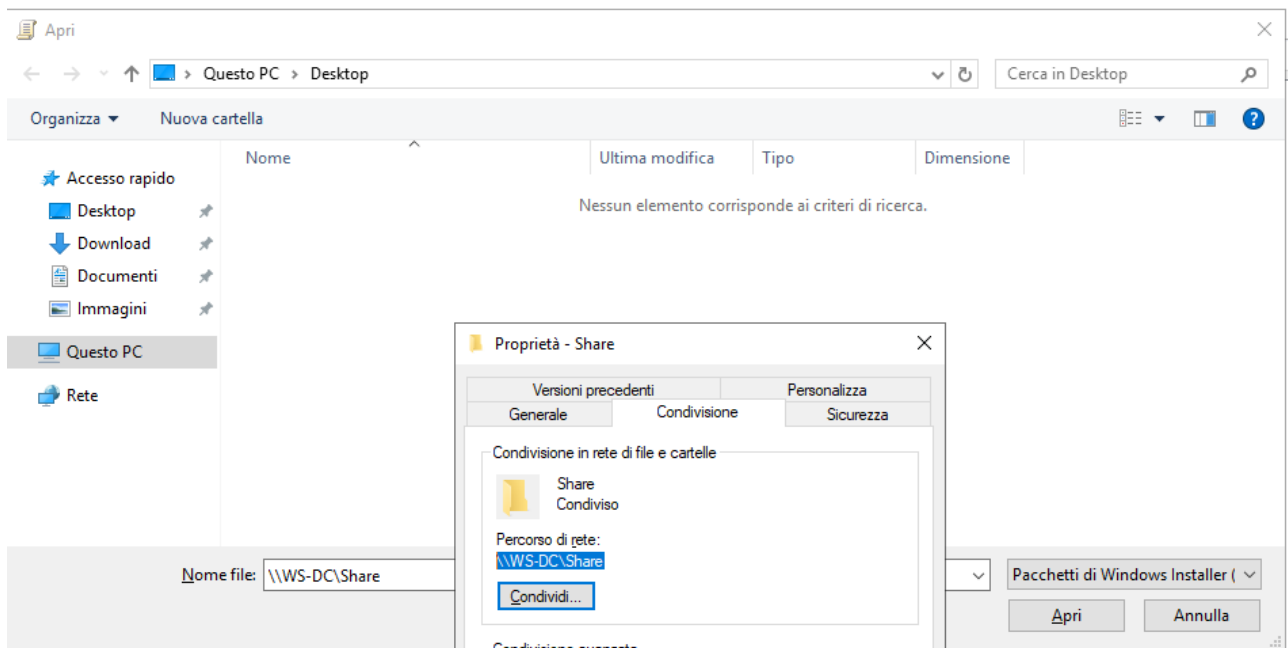
Per distribuire il client potete utilizzare i metodi che preferite, sia con l'installazione manuale che con la distribuzione tramite Group Policy client-side extension o con altri metodi ESD (Electronic Software Distribution).

Tramite Group Policy

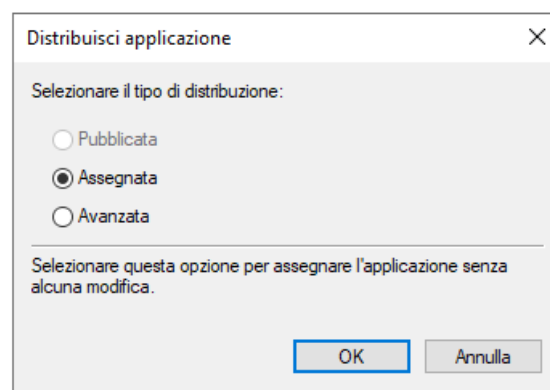
1. Creare una cartella con all'interno il file e condividerla in rete
2. Creare/Aggiungere la GPO nella medesima OU dedicata **Computer Configuration**→**Policies**→**Software Settings**→**Software installation** Tasto dx → **Nuovo** → **Pacchetto**



3. Nella nuova inserire il path della cartella condivisa che troviamo nella scheda di condivisione e facciamo doppio click sul file



4. Selezionare la voce Assegna e confermare



Procedete quindi all'installazione del software e, nel caso l'abbiate fatta manualmente, ricordatevi di aggiornare le policy con il comando **gpupdate /force**.

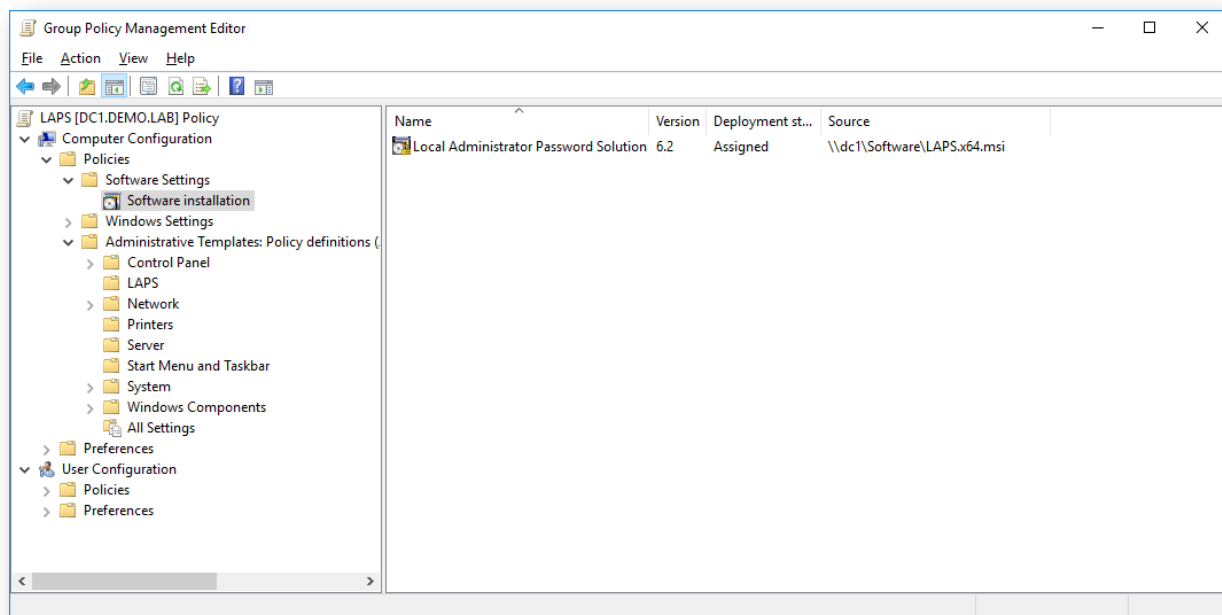


Figura 6: Distribuzione del client LAPS tramite GPO

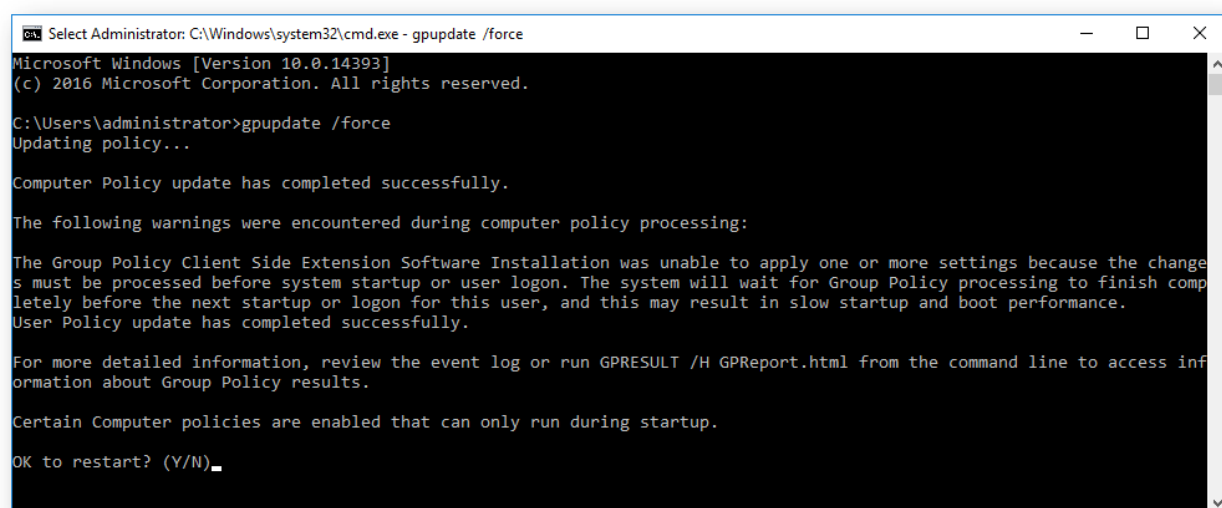


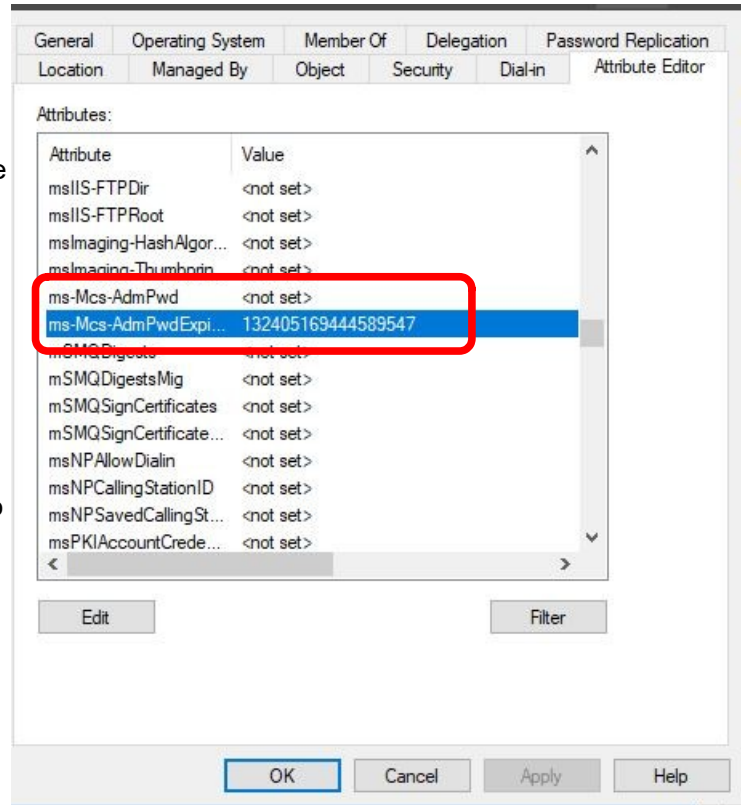
Figura 7: Applicazione della GPO sui pc client

Operazioni aggiuntive per garantire il successo

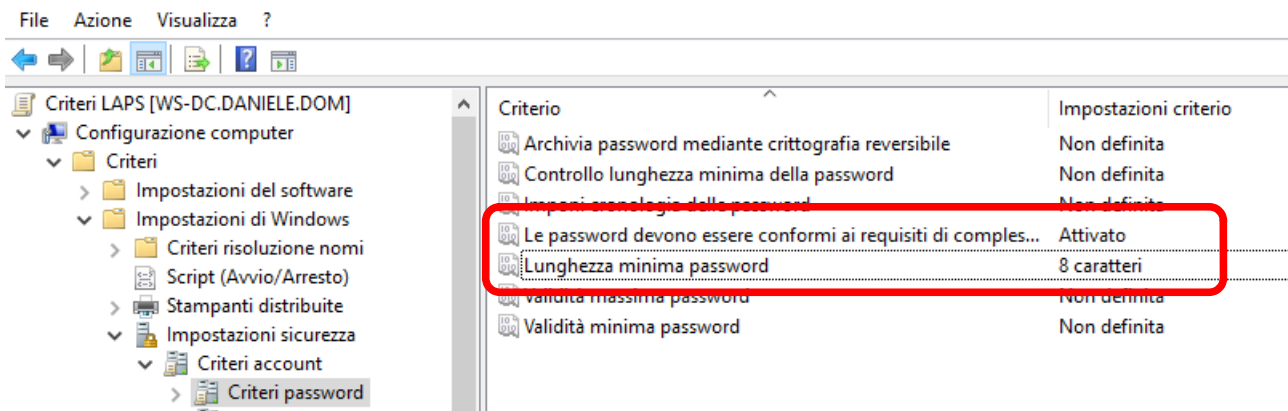
Potrebbe capitare in alcuni casi che, nonostante la corretta installazione, LAPS imposti la data di scadenza ma non restituisca alcuna password, questo è verificabile nella scheda Editor Attributi nelle proprietà del Computer dove troveremo

- ms-Mcs-Adm-Pwd <not set>
- ms-Mcs-AdmPwdExpirationTime

Se è così il problema potrebbe essere causato dalla politica delle password, quando il criterio password in LAPS è meno complesso del criterio password predefinito locale nei client oppure la politica di default non viene ereditata correttamente.



Per aggirare tale problema si può provare a creare una nuova politica delle password interna alla stessa OU come segue di seguito.



Dopo di che lanciamo nuovamente il comando `gpupdate /force` sul DC e sui client

Fonte: [LAPS Not showing password | Microsoft Learn](#)

Creazione password temporanea

Dopo aver riavviato il client per permettere l'installazione dell'agent di LAPS, potete tornare sul vostro server di amministrazione (nel mio caso il domain controller) e da **Start** aprire **LAPS UI**.

Digitate il nome del computer da ricercare e fate clic su **Search**. Vi apparirà la password dell'amministratore locale e la scadenza, come mostrato in figura:

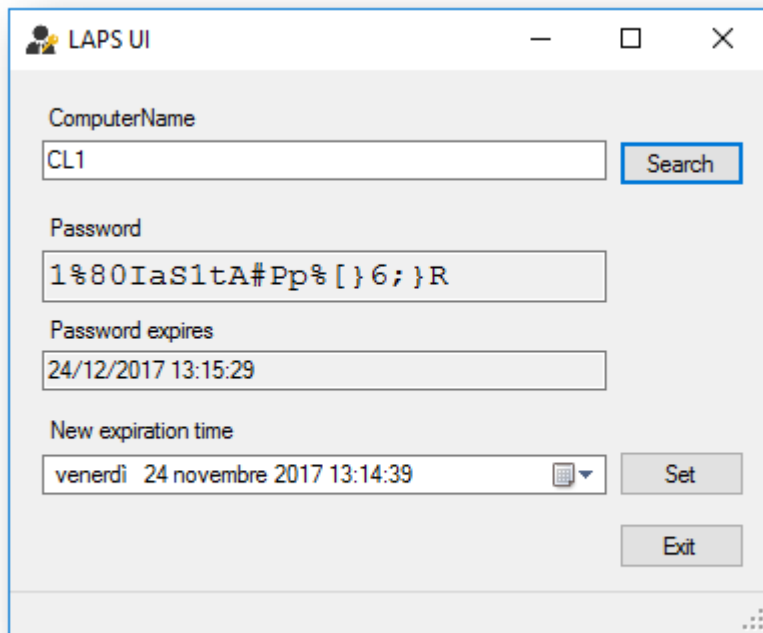


Figura 8: Verifica della password tramite LAPS UI

In alternativa all'interfaccia grafica è anche possibile utilizzare la cmdlet [Get-AdmPwdPassword CL1 | Out-GridView](#)

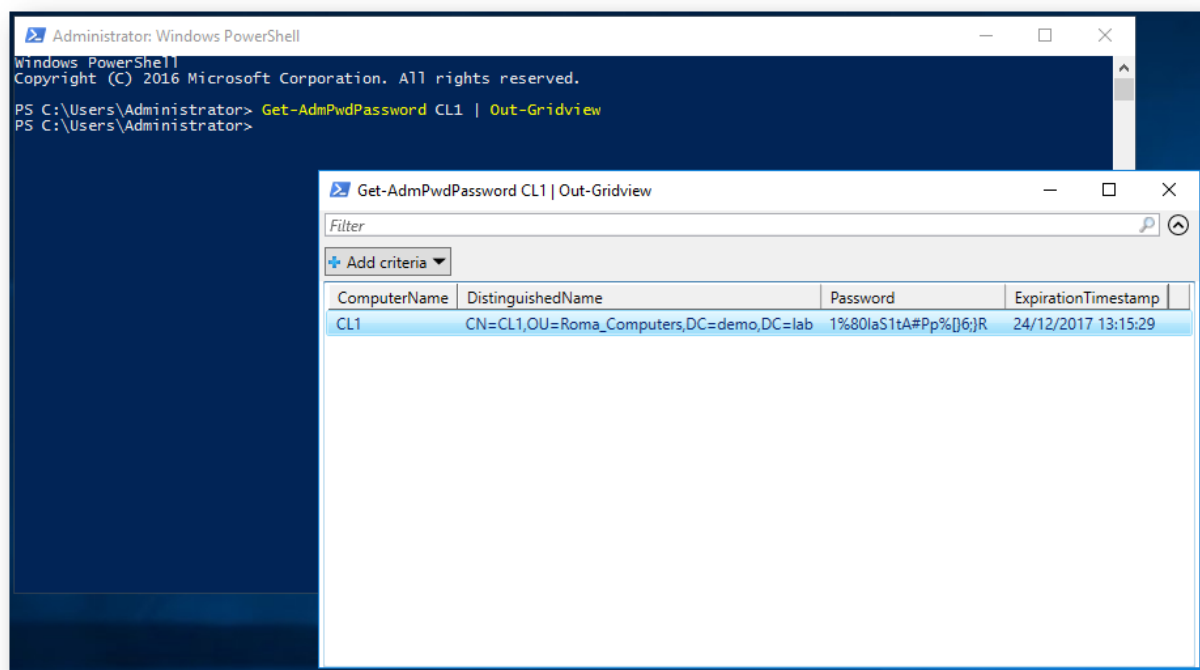


Figura 9: Utilizzo di PowerShell per la visualizzazione della password

Oppure è possibile visualizzare il valore dell'attributo **ms-Mcs-AdmPwd** del Computer Account in modalità visualizzazione avanzata della console di Active Directory Users and Computers.

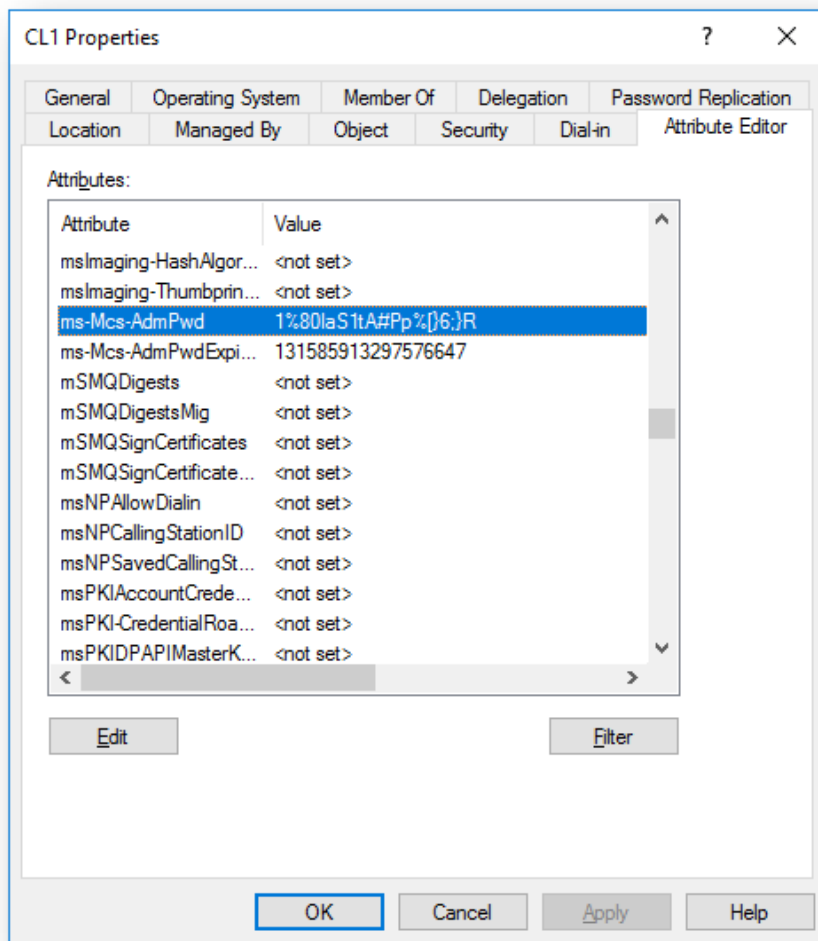


Figura 10: Attributo ms-Mcs-AdmPwd del computer account in AD

Per permettere ai computer di poter aggiornare la password dell'amministratore locale quando scade è sufficiente eseguire con privilegi elevati la cmdlet di Powershell `Set-AdmPwdComputerSelfPermission -Identity "Roma_Computers"`

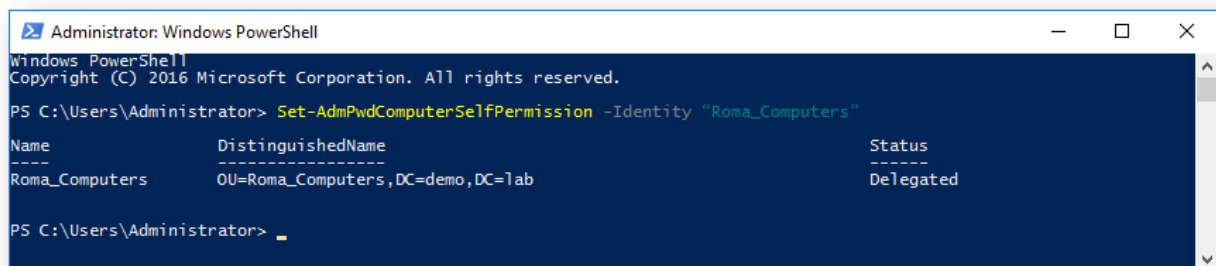
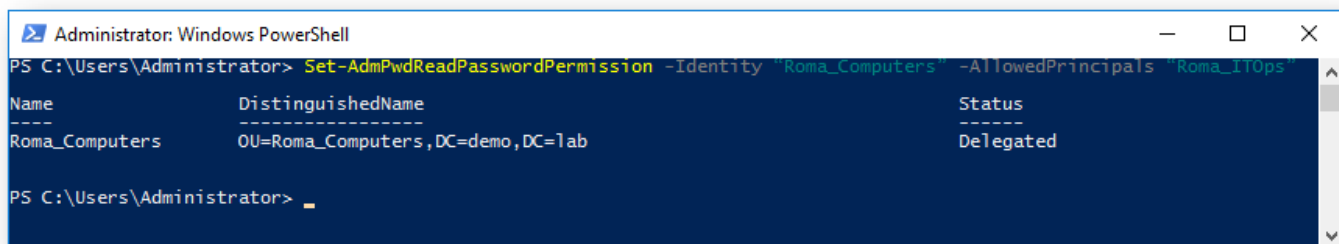


Figura 11: Abilitazione per l'autoaggiornamento della password

Per impostazione predefinita i gruppi Domain Admins ed Enterprise Admins possono visualizzare le password gestite tramite LAPS. Se volete delegare ad un gruppo specifico la possibilità di vedere le password dell'amministratore locale allora sarà necessario eseguire con privilegi elevati la cmdlet di Powershell `Set-AdmPwdReadPasswordPermission -Identity "Roma_Computers" -AllowedPrincipals "Roma_ITOps"`



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Set-AdmPwdReadPasswordPermission -Identity "Roma_Computers" -AllowedPrincipals "Roma_ITOps"

Name           DistinguishedName           Status
----           -
Roma_Computers OU=Roma_Computers,DC=demo,DC=lab Delegated

PS C:\Users\Administrator>
```

Figura 12: Delega amministrativa per LAPS

Conclusioni

Local Administrator Password Solution (LAPS) permette di semplificare enormemente la gestione delle password degli amministratori locali e soprattutto aumenta il livello di sicurezza delle postazioni di lavoro. Molto spesso l'utilizzo della stessa password, che si ripete da diversi anni, è una vulnerabilità sensibile delle nostre macchine e le espone alla possibilità di essere facilmente attaccate o di essere amministrate da utenti non autorizzati.

Maggiori informazioni le trovate al link <https://technet.microsoft.com/it-it/mt227395.aspx>