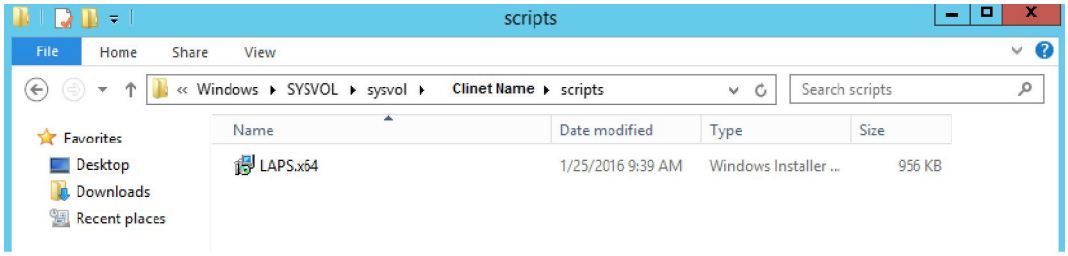
Microsoft Local Administrator Password Solution (LAPS)

اطلقت مايكروسوفت أداة تسمى Local Administrator Password Solution (LAPS)يمكنك من خلالها تغير Local Administrator Password لجميع الاجهزة فى بيئة الدومين بطريقة اتوماتيكيه ومايميز هذه الاداة هى سهولة استخدمها بدون الدخول فى تعقيدات كتابه اسكربت او أستخدام اكثر من اداة للقيام بتغيير الباسورد لجميع الاجهزة فى بيئه الدومين بطريقه اتوماتيكيه غير انها توفر جميع شروط حمايه الباسورد من الاختراق brute force attack وتحديد صلاحيات من يستطيع معرفه الباسورد الجديده كما سوف نرى لاحقا

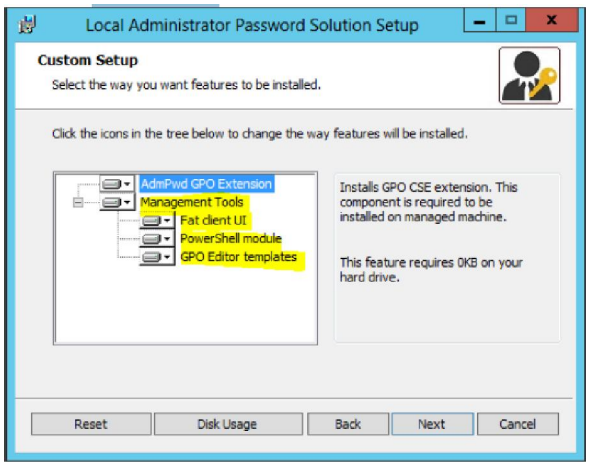
Local Administrator Password Solution (LAPS) هى أداة مجانية ويمكنك تحميلها من هنا

طريقة الاعداد

بعد تحميل الأداة من اللينك السابق سوف نقوم بالدخول على الدومين كنترولر ونقوم بنسخ الأداة بداخل NETLOGON Folder وسوف تجد NETLOGON Folder فى هذا المسار NETLOGON Path:
C:\Windows\SYSVOL\sysvol\ConetDomainName\scripts
ملحوظه : LAPS Tools تحتاج الى Microsoft .NET Framework 4.0



بعد ذلك تقوم بعمل سطب للأداة على الدومين كنترولر ونقوم بتنزيل جميع محتويتهاFull installation



بعد ذلك نقوم بعمل 2 Security Groups فى Active Directory

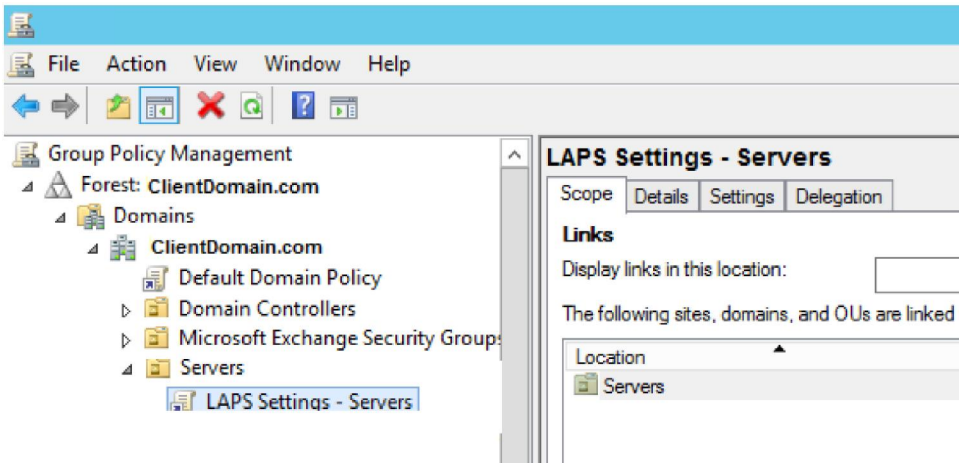
" LAPS Admins – Servers , LAPS Exceptions – Servers "

LAPS Admins – Servers: هى الجروب التى سوف نقوم من خلالها بتحديدLAPS Tools Administrator

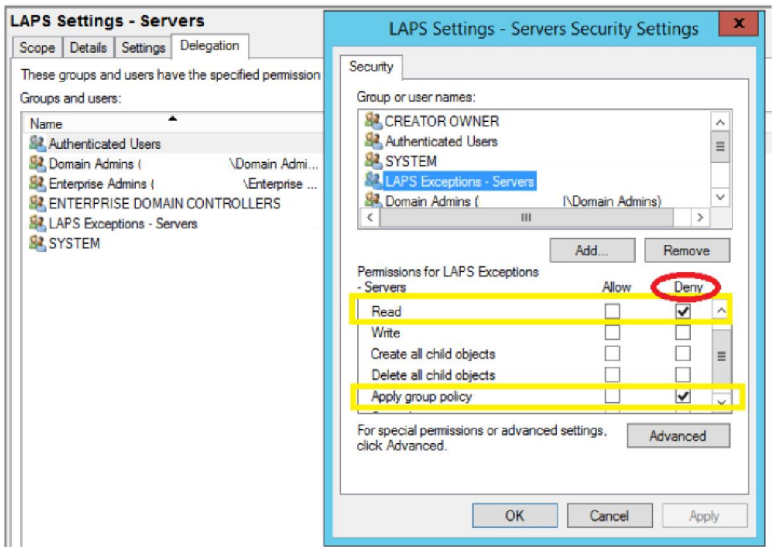
LAPS Exceptions – Servers: هى الجروب التى سوف نقوم من خلالها بتحديد اى كمبيوتر لا نريد تطبيق هذة الاداة عليه

LAPS Admins - Servers	Security Group...	Admins who can Access LAPS Tool
LAPS Exceptions - Servers	Security Group...	Servers Needs to be execluded form LAPS comes here

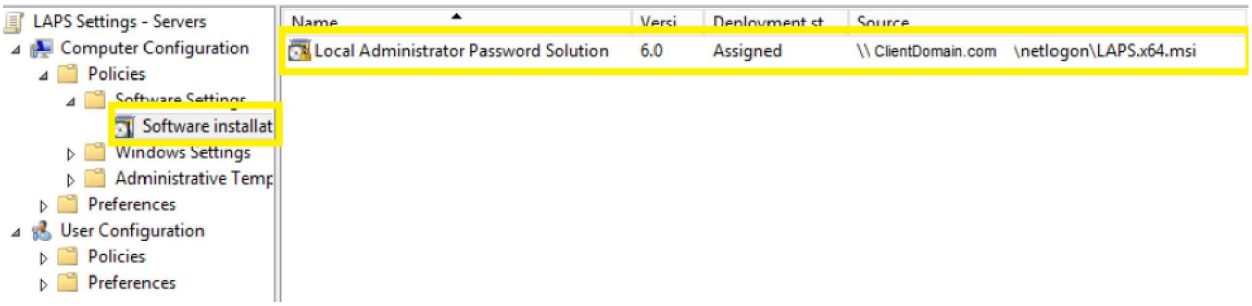
بعد ذلك سوف نقوم بعمل Group Policy نقوم من خلالها بعمل الاعدادت المطلوبه سوف اقوم بتسميتها LAPS Settings – Servers لان فى هذا اللاب اقوم بتطبيق الأداة على Servers فقط ويمكن تطبيقها على جميع الأجهزة فى بيئة الدومين فبدل انت تقوم بعمل Link Policy على OU معينهيمكنك عمل Link على الدومين لتطبيقها على جميع الاجهزة



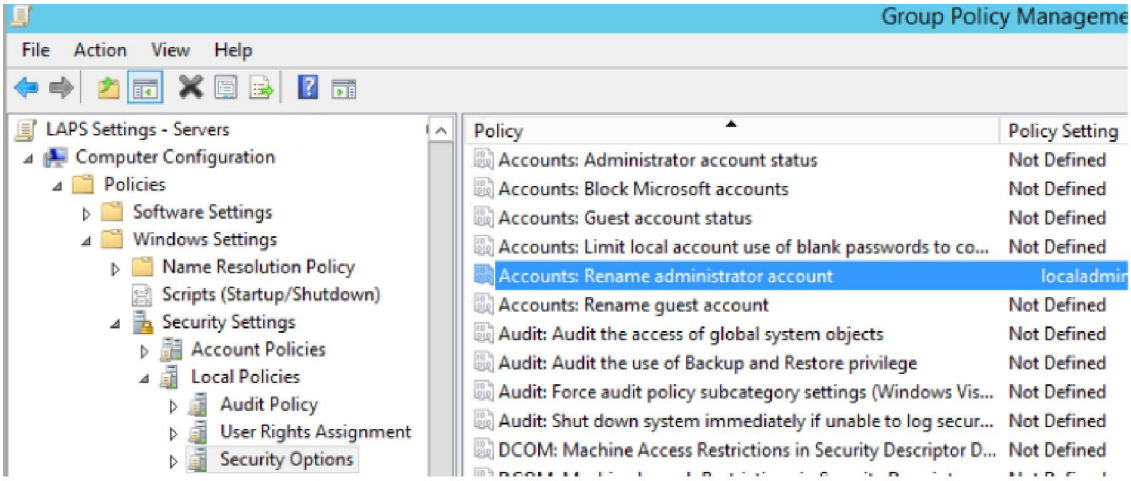
قبل الدخول فى اعدادت الجروب بوليسى سوف اقوم أولاً باضافة LAPS Exceptions – Servers Group فى جزئية Delegation ونقوم بتحديد البرميشن الاتيه Deny Read and Don't Apply settingsكما هو موضوح بالصوره



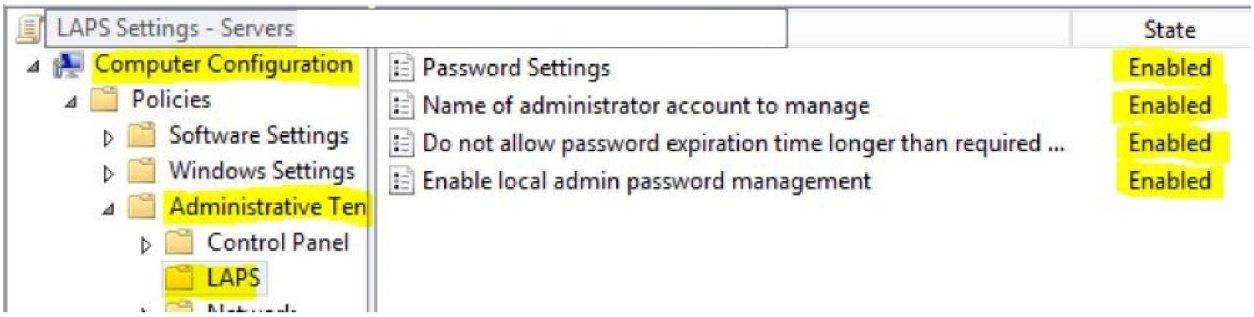
الان سوف نقوم بعمل اعدادات الجروب البولسى سوف نقوم اولاً بعمل سطب للأداة على جميع السرفير عن طريق الجروب بوليسى من جزئيه Software Installation كما هو موضوح بالصوره التاليه



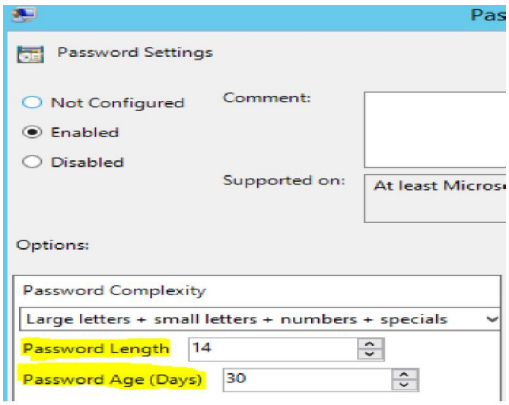
بعد ذلك سوف اقوم بتغير اسم Local Administrator User الى localadmin وهذة الخطوه اختياريه وليست اجباريه ويمكنك تغير الاسم الى اى اسم انت تريده او يمكنك تركه على الاسم الافتراضى Administrator ولكن يفضل تغير الاسم لزياده مستوى الامان ويمكن تغير اسم Local Administrator User عن طريق Group Policy كما هو موضح بالصوره التاليه



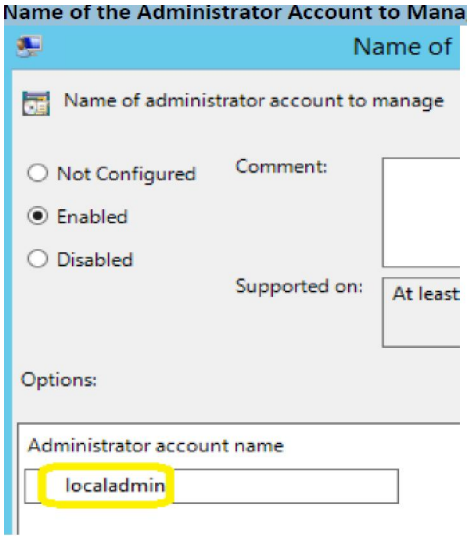
بعد ذلك نقوم بعمل الاعدادت الخاصه بأداة LAPS عن طريق الجروب بوليسى وسوف تجدها فى هذا المسار Computer Configuration > Administrative Templet > LAPS كما هو موضوح بالصوره



Password Settings: سوف نقوم من خلال هذه البولسى بتحديد مكونات الباسورد بمعنى فى هذا الامثال الباسورد سوف تتكون من حروف كبيره وحروف صغيره وارقام ورموز ويكون طول الباسورد مكون من 14 حرف ويقوم بتغيير الباسورد كل 30 يوم ويمكنك تحديد هذة الخيارات حسب ماينا‌سبك ويناسب طبيعه عملك

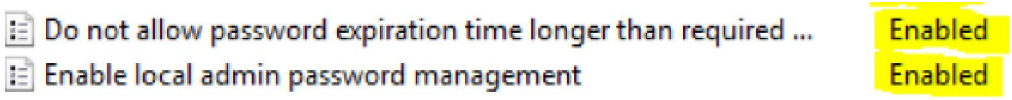


Name of the Administrator Account to Manage: سوف نقوم من خلال هذة البولسى بتحديد اسم User Account الذي سوف يقوم بتطبيق الاعدادت عليه فى هذا المثال سوف نكتب localadmin ولو لم تقوم بتغير اسم Local Administrator user سوف تكتب الاسم الافتراضى Administratorاو الاسم الذى قمت بتغيره



وسوف نقوم ايضاً بعمل Enable لكلا من

- **Do Not allow password expiration time longer than required**
- **Enable local admin password Management**



فى اخر مرحله سوف نقوم بتطبيق بعض Power Shell Commands

اولاً سوف نقوم بتحديث Active Directory Schema عن طريق الامر

```
Import-Module AdmPwd.PS

Update-AdmPwdADSchema
```

ملحوظه : لابد من تطبيق Power Shell Commands على الدومين كنترولر الذي يقوم بدور Schema Operation Master Role

```
PS C:\Windows\system32> Import-Module AdmPwd.PS
PS C:\Windows\system32> Update-AdmPwdADSchema
```

بعد ذلك سوف نقوم بتحديد صلاحيات من يستطيع مشاهده معرفه الباسورد عن طريق الأداة LAPS ويمكن فى هذة النقطة عمل جروب اخرى تسطيع من خلالها تحديد من يقوم بقراءه الباسورد فقط ولكن لا يستطيع تعديل اى اعدادات ولكن فى هذا المثال سوف اقوم باستخدم نفس جروب LAPS Admins – Servers

Set-AdmPwdReadPasswordPermission–Identity “Servers” –AllowedPrinciapals “LAPS Admins – Servers”

Set-AdmPwdReadPasswordPermission : كما هو واضح من الاسم هو الامر الذى يحدد ReadPasswordPermission

Identity: هو الذى من خلاله نقوم بتحديد OU او اسم DC

AllowedPrinciapals : هو الذى نقوم من خلاله بتحديد اسم الجروب

```
PS C:\Windows\system32> Set-AdmPwdReadPasswordPermission -Identity "Servers" -AllowedPrincipals "LAPS Admins - Servers"

Name                DistinguishedName                                     Status
----                -----------------                                     ------
Servers             OU=Servers,DC=Imagenation,DC=ae                       Delegated
```

سوف نقوم بعد ذلك بتحديد صلاحيات من يستطيع تغير الباسورد وفى هذا المثال سوف استخدم نفس الجروب LAPS Admins – Servers

ويمكن استخدام جروب اخر كما وضحت سابقا

Set-AdmPwdResetPasswordPermission –Identity “Servers” –AllowedPrinciapals “LAPS Admins – Servers”

AdmPwdResetPasswordPermission : كما هو واضح من الاسم هو الامر الذى يحدد Reset PasswordPermission

Identity: هو الذى من خلاله نقوم بتحديد OU او اسم DC

AllowedPrinciapals : هو الذى نقوم من خلاله بتحديد اسم الجروب

```
PS C:\Windows\system32> Set-AdmPwdResetPasswordPermission -Identity "Servers" -AllowedPrincipals "LAPS Admins - Servers"

Name                DistinguishedName                                     Status
----                -----------------                                     ------
Servers             OU=Servers,DC=Imagenation,DC=ae                       Delegated
```

فى هذا الامر سوف نقوم باعطاء Computer Objects صلاحيات مطلوبه على OU او اسم الدومين

```
Set-AdmPwdComputerSelfPermission –Identity “Servers”
```

```
PS C:\Windows\system32> Set-AdmPwdComputerSelfPermission -Identity "Servers"
```

فى اخر امر ونكون انتهينا هو تفعيل خصيه Audit فى حاله قراءة او تغيير الباسورد

```
Set-AdmPwdAuditing –Orgunit “Servers” –AuditedPrincipals “Authenticated Users”
```

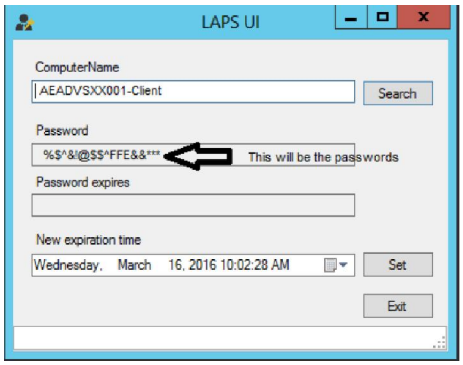
Set-AdmPwdAuditing : كما هو واصح من الاسم هو الامر المسؤل عن تفعيل خاصية Audit

Orgunit : هو من خلال بقوم تحديد OU

AuditPrincipals : هة الذى استطيع من خلال تحديد الجروب وتم اختيار الجروب Authenticated Users حتى يقوم بمراقبة جميع اليوزر فى الدومين الموجودين حالياً او الذى سوف نقوم بانشاءهم

```
PS C:\Windows\system32> Set-AdmPwdAuditing -OrgUnit "Servers"-AuditedPrincipals "Authenticated Users"
```

الان قد انتهينا من جميع الاعدادت المطلوبه وفى حاله معرفه الباسورد سوف تقوم بفتح LAPS GUI Tools ووضع اسم الجهاز وسوف تقوم الاداة بعرض الباسورد امامك ولكن سوف يستطيع مشاهدة الباسورد فقط كل من هم بداخل الجروب LAPS Admins – Servers



اتمنى ان المقال ينال اعجباكم وانتظرونى فى مقال اخر ان شاء الله قريبا وكل عام وانتم بخير بمناسبة حلول شهر رمضان الكريم ولا تنسونى من خالص دعائكم

م/ محمود عاطف