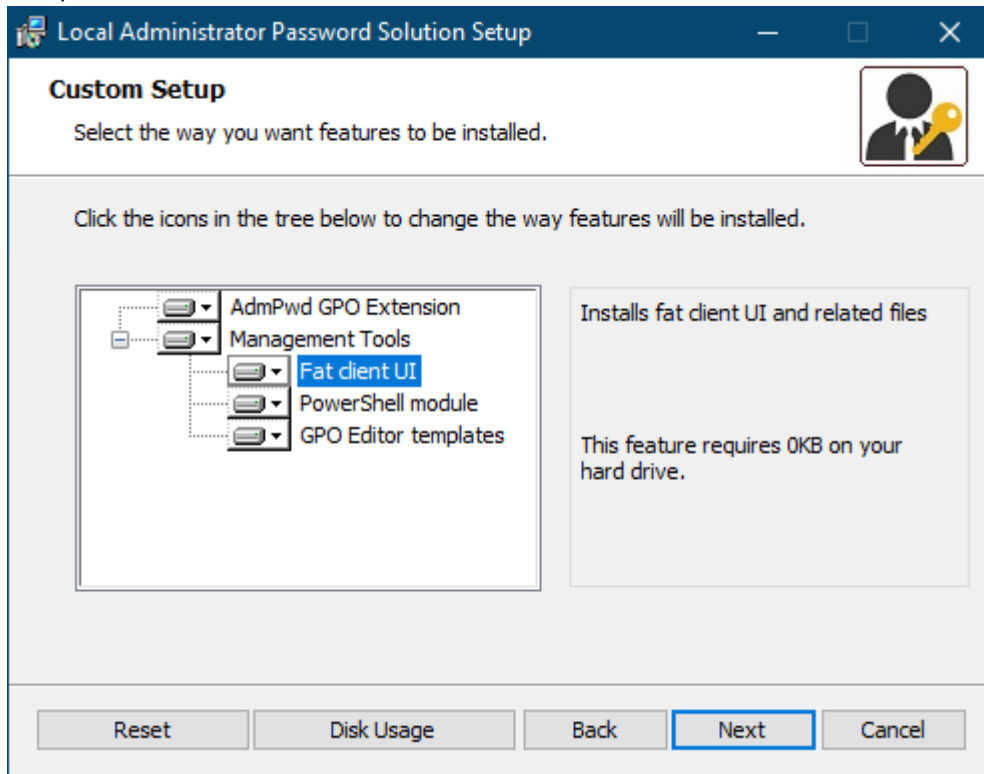


1. Runterladen des Clients: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>
2. Installieren auf dem DC. Wichtig darauf achten zumindest die PowerShell Module und GPO Templates zu installieren



3. Update des AD Schema

```
Update-AdmPwdADSchema
```

4. Update der Berechtigung das die Computerkonten innerhalb der OU „Struktur“ die gerade erweiterten AD Attribute schreiben dürfen

```
Set-AdmPwdComputerSelfPermission -OrgUnit "Struktur"
```

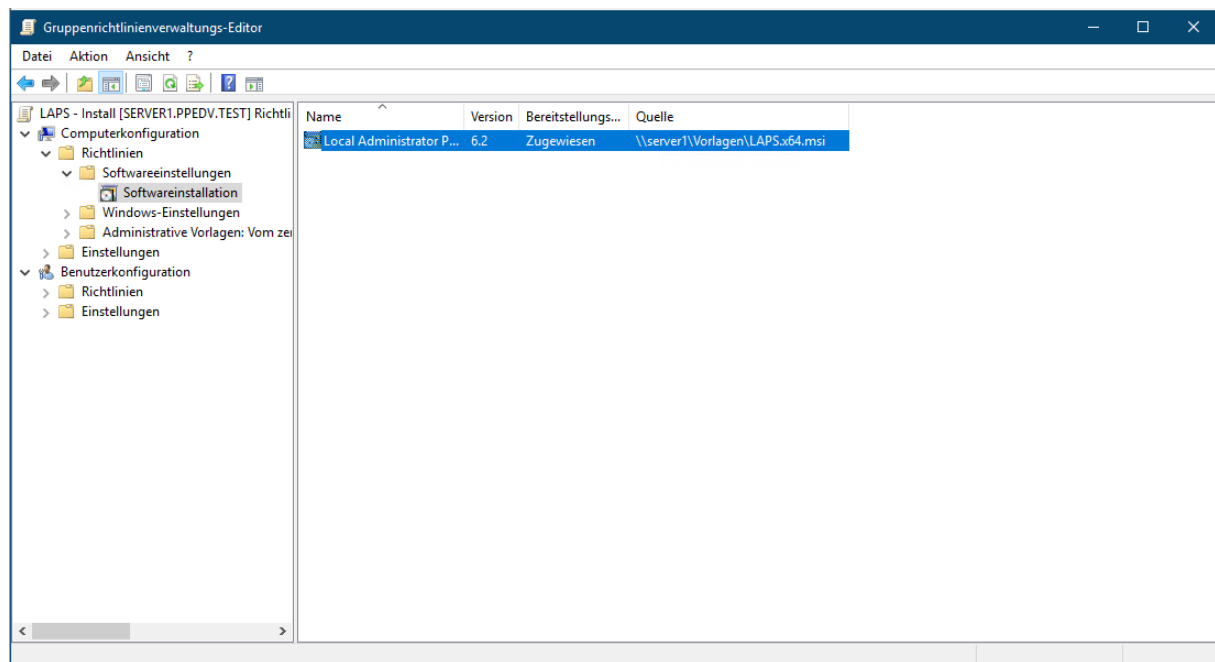
- 5.
6. Setzen der Berechtigung das die DomainLocal Group „DL-LAPS“ die Passwörter Lesen und zurücksetzen darf. Diese Gruppe könnte unter Verwendung des AGDLP Schemas, welches RBAC ähnelt verwendet werden um das Recht an einen Helpdesk zu delegieren

```
Set-AdmPwdReadPasswordPermission -OrgUnit "Struktur" -AllowedPrincipals "DL-LAPS"
```

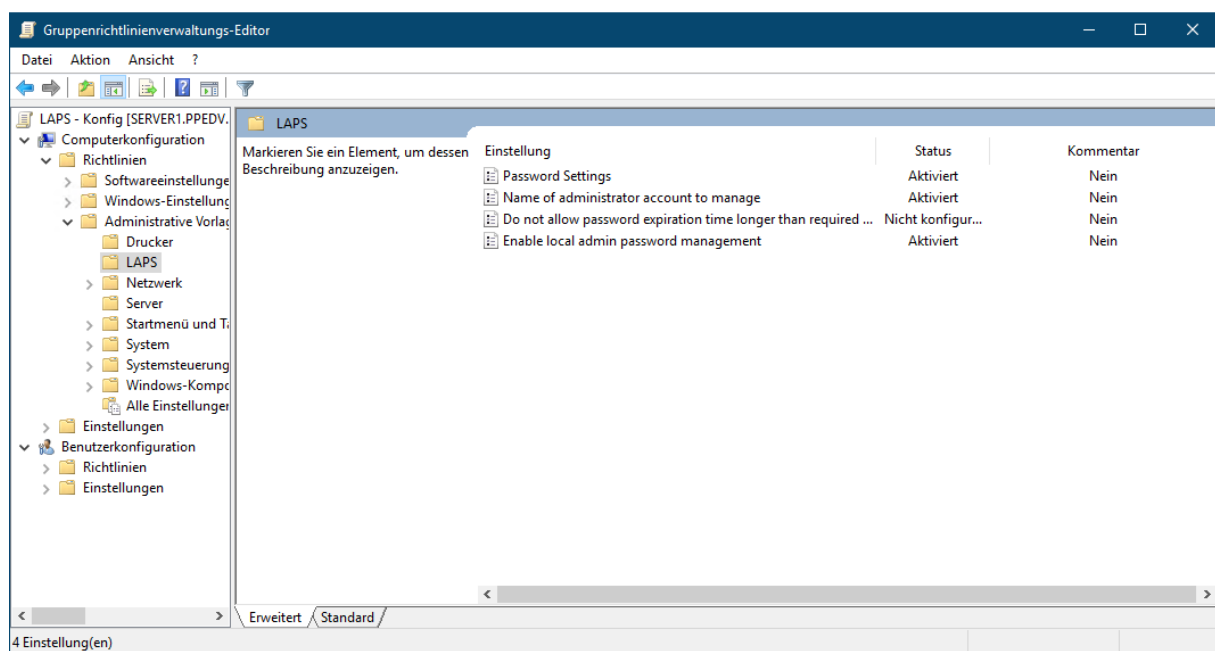
- 7.
8.

```
Set-AdmPwdResetPasswordPermission -OrgUnit "Struktur" -AllowedPrincipals "DL-LAPS"
```

9. Ablegen der MSI Datei auf einem erreichbaren FileShare
10. Anlegen der Gruppenrichtlinie zur Installation der Anwendung



11. Bei Verwendung des
12. Anlegen der Gruppenrichtlinie zur Konfiguration



Windows Password Settings

Password Settings Vorherige Einstellung Nächste Einstellung

☐ Nicht konfiguriert Kommentar:

☒ Aktiviert

☐ Deaktiviert

Unterstützt auf:

Optionen: Hilfe:

Password Complexity

Large letters + small letters + numbers + specials

Password Length

Password Age (Days)

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

OK Abbrechen Übernehmen

Windows Name of administrator account to manage

Name of administrator account to manage Vorherige Einstellung Nächste Einstellung

☐ Nicht konfiguriert Kommentar:

☒ Aktiviert

☐ Deaktiviert

Unterstützt auf:

Optionen: Hilfe:

Administrator account name

Administrator account name: name of the local account you want to manage password for.
DO NOT configure when you use built-in admin account. Built-in admin account is auto-detected by well-known SID, even when renamed

DO configure when you use custom local admin account

OK Abbrechen Übernehmen

Enable local admin password management

Enable local admin password management

Vorherige Einstellung

Nächste Einstellung

☐ Nicht konfiguriert

☒ Aktiviert

☐ Deaktiviert

Kommentar:

Unterstützt auf:

At least Microsoft Windows Vista or Windows Server 2003 family

Optionen:

Hilfe:

Enables management of password for local administrator account

If you enable this setting, local administrator password is managed

If you disable or not configure this setting, local administrator password is NOT managed

OK

Abbrechen

Übernehmen

13. Auf den Clients (Computerkonten müssen sich in der richtigen OU befinden) „gpupdate /force“ ausführen. Neustarten zur Installation des Clients. Nach dem neustart „gpupdate /force“, neustarten und jetzt sollte das Passwort des lokalen „Admin“ Accounts im AD stehen

BitLocker-Wiederherstellung

Einwählen

Sicherheit

Standort

Kennwortreplikation

Attribut-Editor

Attribute:

Attribut	Wert
lastLogoff	(nie)
lastLogon	11.06.2021 15:15:34 Mitteleuropäische Sommerzeit
lastLogonTimestamp	10.06.2021 14:48:35 Mitteleuropäische Sommerzeit
localPolicyFlags	0
logonCount	46
msDS-SupportedEncryptionMethods	0x1C = (RC4_HMAC_MD5 AES128_CTS_HMAC_SHA1)
ms-Mcs-AdmPwd	1h8d[(SW
ms-Mcs-AdmPwdExpirationTime	132704829342836430
name	CLIENT1
objectCategory	CN=Computer,CN=Schema,CN=Configuration,DC=com
objectClass	top; person; organizationalPerson; user; computer
objectGUID	1255be89-748f-4de0-922f-f8c6b96dd2ea
objectSid	S-1-5-21-3129317790-3302870524-4458206
operatingSystem	Windows 10 Education

Bearbeiten

Filter