



Computerkonto Kennwortalter

Das Computer-Kennwort authentifiziert ein Computerkonto genauso wie der Benutzername und das dazugehörige Kennwort eines Benutzers.

Benutzerkennwörter laufen in der Regel mittlerweile nach 90 Tagen aus. Bei einem Computerkonto, sofern man diese Richtlinie nicht angefasst hat nach 30 Tagen.

Das ist in einer Produktionsumgebung auch korrekt. In einer Testumgebung kann das hinderlich sein. Denn hier werden die Maschinen auch schon mal über eine längere Zeit heruntergefahren.

Was passiert, wenn eine Maschine länger down war und dann gestartet wird, oder eine Maschine aus dem Backup zurückgespielt wird? Die Kennwörter können unterschiedlich sein. Das Computerkontokennwort, mit dem im Active Directory gespeicherten Kennwort kann muss aber nicht unterschiedlich sein.

Folgende Hinweismeldungen können z.B. angezeigt werden:

Die Vertrauensstellung zwischen dieser Arbeitsstation und der primären Domäne konnte nicht hergestellt werden.

The trust relationship between this workstation and the primary domain failed.

This Computer was not able to set up a secure session with a domain controller in domain dwp.local due to the following: There are currently no logon servers available to service the logon request.

This Computer was not able to set up a secure session with a domain controller in domain dwp.local due to the following: The remote procedure call was cancelled. This may lead to authentication problems.

There are currently no logon servers available to service the logon request

Vorgehen:

Entweder man meldet sich lokal mit dem Administratorkonto an und setzt in der Powershell oder CMD folgende Befehle ab, um das Kennwort zu resettten:

```
Reset-ComputerMachinePassword -Server DC01 -Credential ndsedv\admin  
Test-ComputerSecureChannel -Server DC01 -Credential ndsedv\admin
```

```
netdom resetpwd /s: dc01 /ud:NDS /pd: Passwort  
nltest /sc_query:ndsedv
```

Mögliche Empfehlung für eine Testumgebung:

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen\Domänenmitglied

Änderung von Computerkennwörtern deaktivieren

Standard=nicht definiert
Neuer Wert = deaktiviert

Maximalalter von Computerkontenkennwörtern

Standard=nicht definiert
Neuer Wert = 90



Computerkonto Kennwortalter

Ansicht der Optionen

Bitte aktiviert niemals die erste Option, denn diese Deaktiviert die Kennwortänderung und macht das System für Passthrough Angriffe verwundbar. Ein Computerkennwort* wird für die sichere Kommunikation (Secure Channel) z.B. mit einem DC verwendet.

Richtlinie	Richtlinieneinstellung
Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Admin...	Nicht definiert
Benutzerkontensteuerung: Alle Administratoren im Administratorgenehmigungsmodus ...	Nicht definiert
Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfo...	Nicht definiert
Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sichere...	Nicht definiert
Benutzerkontensteuerung: Datei- und Registrierungs-schreibfehler an Einzelbenutzerstand...	Nicht definiert
Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicher...	Nicht definiert
Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überpr...	Nicht definiert
Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sichere...	Nicht definiert
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Ad...	Nicht definiert
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Sta...	Nicht definiert
DCOM: Computerstarteinschränkungen in Security Descriptor Definition Language (SDD...	Nicht definiert
DCOM: Computerzugriffseinschränkungen in Security Descriptor Definition Language (S...	Nicht definiert
Domänencontroller: Änderungen von Computerkontenkennwörtern verweigern	Nicht definiert
Domänencontroller: Serveroperatoren das Einrichten von geplanten Aufgaben erlauben	Nicht definiert
Domänencontroller: Signaturanforderungen für LDAP-Server	Nicht definiert
Domänenmitglied: Änderungen von Computerkontenkennwörtern deaktivieren	Deaktiviert
Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)	Nicht definiert
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)	Nicht definiert
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Nicht definiert
Domänenmitglied: Maximalalter von Computerkontenkennwörtern	90 Tage
Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher)	Nicht definiert
Geräte: Anwenden des Installieren von Drucktreibern nicht erlauben	Nicht definiert
Geräte: Entfernen ohne vorherige Anmeldung erlauben	Nicht definiert
Geräte: Formatieren und Auswerfen von Wechselmedien zulassen	Nicht definiert
Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Nicht definiert
Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Nicht definiert
Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeichers löschen	Nicht definiert
Herunterfahren: Herunterfahren des Systems ohne Anmeldung zulassen	Nicht definiert
Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum Ändern des Kennworts...	Nicht definiert
Interaktive Anmeldung: Anzahl zwischenzuspeicherter vorheriger Anmeldungen (für de...	Nicht definiert
Interaktive Anmeldung: Benutzerinformationen anzeigen, wenn Sitzung gesperrt ist	Nicht definiert
Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrun...	Nicht definiert
Interaktive Anmeldung: Inaktivitätsgrenze des Computers	Nicht definiert
Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich	Nicht definiert
Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen	Nicht definiert
Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen	Nicht definiert

Nach Übernahme der Richtlinieneinstellungen sehen die Werte in der Registry wie folgt aus:

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
DisablePasswordChange	REG_DWORD	0x00000000 (0)
DynamicSiteName	REG_SZ	Default-First-Site-Name
MaximumPasswordAge	REG_DWORD	0x0000005a (90)
RequireSignOrSeal	REG_DWORD	0x00000001 (1)
RequireStrongKey	REG_DWORD	0x00000001 (1)
SealSecureChannel	REG_DWORD	0x00000001 (1)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\netlogon.dll
SignSecureChannel	REG_DWORD	0x00000001 (1)
Update	REG_SZ	no



Computerkonto Kennwortalter

*Beim Hinzufügen eines Computers zu einer Domäne wird ein Computerkonto erstellt. Wenn der Computer anschließend gestartet wird, verwendet er das Kennwort des Computerkontos, um einen sicheren Kanal mit einem Domänencontroller aufzubauen.

Dieser sichere Kanal wird verwendet, um Vorgänge wie die NTLM-Passthrough-Authentifizierung, LSA/SID-Namenssuche usw. auszuführen.

Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)	Nicht definiert
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)	Nicht definiert
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Nicht definiert

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]  
"MaximumPasswordAge"=dword:0000005a
```

Dieser Registry-Eintrag konfiguriert das Intervall (15 Minuten) in welchen Abständen das Alter des Computerkennworts überprüft werden soll. Das Intervall kann bis zu 48 Stunden eingestellt werden. Die Einstellung findet in Sekunden statt und in Dezimal.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters]  
"ScavengeInterval"=dword:00000384
```

Dieser Eintrag schaltet die Funktion das ein Computerkennwort benötigt wird ein.

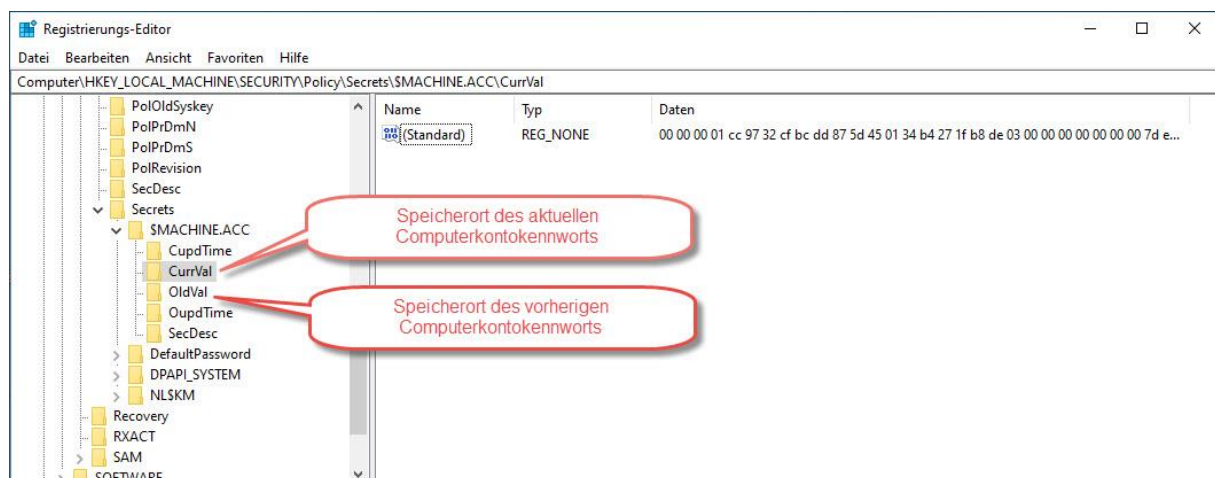
Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]  
"DisablePasswordChange"=dword:00000000
```

Computerkennwörter werden in der Registry an dieser Stelle gespeichert:

```
HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets\SMACHINE.ACC\CurrVal
```

```
psexec -i -d -s regedit
```



Weitere Informationen zum Thema Probleme mit Secure Channel.



Computerkonto Kennwortalter

<https://www.der-windows-papst.de/2020/11/19/netlogon-event-5719-oder-5783/>