Lokaler Administrator zurücksetzen

Lokaler Administrator zurücksetzen

Wichtig: Vor jedem Bypass/Notfallverfahren prüfen, ob der Kunde über ein Change-Management und explizite Freigabe verfügt. Bypass-Methoden schwächen die Sicherheit des Systems (UAC, Account Lockout, Logging) und sind nur im Verlustfall der einzigen administrativen Zugänge zulässig.

1. Unterstützte Methoden (bevorzugt)

A. Windows LAPS (Windows 11/10, Windows Server 2019+) — bevorzugt

Ist Windows LAPS aktiv (GPO/Intune), kann das rotierte lokale Admin-Passwort vom Client selbst oder aus dem Verzeichnis/Intune gelesen werden:

```
## Lokal auf dem Client auslesen (erfordert Admin-Rechte)
Get-LapsLocalPassword
## Alternativ aus dem AD (Directory auslesen)
Get-LapsADPassword -Identity <COMPUTERNAME> -Domain <domain.tld>
```

Quelle: https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview

B. Zurücksetzen über einen vorhandenen zweiten Admin

Wenn ein anderer Admin-Konto noch existiert, einfach über das Konto oder PowerShell:

```
## Erzwinge Passwortwechsel bei nächster Anmeldung
Set-LocalUser -Name "Administrator" -Password (Read-Host -AsSecureString "Neues Passwort")
## Optional: Account entsperren
Set-LocalUser -Name "Administrator" -PasswordNeverExpires $true
net user Administrator /active:yes
```

C. Via Microsoft Entra ID / Intune

Wenn der Client Entra-joined ist, kann das lokale Admin-Passwort via Windows LAPS oder Intune-Remediation (Proactive Remediation) gesetzt werden.

2. Notfall-/Wiederherstellungsverfahren (nur wenn kein anderer Admin-Zugang möglich)

> ⚠ **Sicherheitswarnung:** Diese Methoden umgehen die Authentifizierung und Loggen. Sie nur mit Kundeneinverständnis und nach dokumentierter Freigabe ausführen.

A. Offline-Editor (z. B. chntpw / Offline NT Password Editor) — Boot von USB

1. Von Linux-USB (z. B. chntpw / Hiren's BootCD) booten.
2. Windows-Partition mounten und `C:\Windows\System32\config\SAM` editieren.
3. Administrator-Passwort auf leer/known setzen und Account wieder aktivieren.

```
## chntpw-Beispiel
sudo chntpw -i /mnt/windows/Windows/System32/config/SAM
```

B. Kon-Boot / alternative Bootloader

Umgeht die Authentifizierung komplett — nur bei guter Zertifizierung der Hardware einsetzen.
Achtung: Kann Secure Boot/BitLocker brechen. Vorher BitLocker-Recovery-Key sichern.

3. Zusätzliche Hinweise

- **BitLocker:** Vor Boot-Manipulationen immer den Recovery-Key (48 Ziffern) verfügbar haben.
- **Microsoft Account:** Wenn der Client Entra-joined/Azure AD-joined ist, kann die lokale Anmeldung via Microsoft Entra ID und Windows LAPS stattfinden.
- **Sicherheit:** Nach jedem Reset sollte das Passwort rotiert, LAPS aktiviert, und ein vollständig dokumentiertes Incident-Report erstellt werden.

Quellen

- Windows LAPS: https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview
- Windows LAPS Cmdlets: https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-powershell-cmdlets
- Get-LapsADPassword: https://learn.microsoft.com/en-us/powershell/module/laps/get-lapsadpassword
- Set-LocalUser: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/set-localuser

---

Quelle: Obsidian `Knowledge Base/Windows/Lokaler Administrator zurücksetzen.md` *· Stand: 2026-10-12 · Automatisiert publiziert durch Hermes.*

Revision #3
Created 2026-10-11 23:34:33 UTC by Hermes
Updated 2026-10-26 22:57:47 UTC by Hermes