

HowTo – Gruppenrichtlinien

Kategorie	Windows Administration
Autor	Lugstein Markus
Datum	14.03.2026
Version	1.0

Inhalt

1. Ziel der Anleitung	2
2. Voraussetzungen.....	2
3. Warnhinweise	2
4. Übersicht der Aufgabe	3
5. Schritt-für-Schritt Anleitung	3
5.1 Schritt 1 – Desktop-Hintergrund festlegen	3
5.2 Schritt 2 – Zugriff auf Systemsteuerung einschränken	4
5.3 Schritt 3 – Windows Update nur manuell.....	4
5.4 Schritt 4 – Passwort-Richtlinie konfigurieren.....	5
5.5 Schritt 5 – USB-Schreibzugriff deaktivieren	5
6. Ergebnis / Kontrolle	6
7. Dokumentation / Abgabe	6
8. Anhang (optional)	7

1. Ziel der Anleitung

Ziel dieser Anleitung ist die Implementierung verschiedener lokaler Gruppenrichtlinien (GPO) auf einem Windows-System.

Die Richtlinien dienen dazu, Unternehmensvorgaben umzusetzen und die Systemsicherheit zu erhöhen. Dazu gehören:

- Festlegen eines Firmenlogos als Desktop-Hintergrund
- Einschränkung des Zugriffs auf die Systemsteuerung
- Kontrolle der Windows Update Einstellungen
- Durchsetzung einer sicheren Passwort-Richtlinie
- Einschränkung des USB-Speicherzugriffs

2. Voraussetzungen

Für die Umsetzung der Gruppenrichtlinien müssen folgende Voraussetzungen erfüllt sein:

- Windows Betriebssystem (z. B. Windows 10 / Windows 11 Pro oder Enterprise)
- Administratorrechte
- Zugriff auf den Lokalen Gruppenrichtlinien-Editor
- Firmenlogo als Bilddatei (z. B. .jpg oder .png)
- Grundkenntnisse in Windows-Systemverwaltung

Der Gruppenrichtlinien-Editor kann mit folgendem Befehl geöffnet werden:

```
gpedit.msc
```

3. Warnhinweise

⚠ Das Ändern von Gruppenrichtlinien kann das Verhalten des Systems erheblich beeinflussen.

Daher sollte beachtet werden:

- Änderungen nur mit Administratorrechten durchführen
- Richtlinien sorgfältig überprüfen
- Vor größeren Änderungen ein Backup oder Wiederherstellungspunkt erstellen

4. Übersicht der Aufgabe

Folgende Gruppenrichtlinien sollen implementiert werden:

Bereich	Einstellung
Desktop	Firmenlogo als Hintergrundbild (gesperrt)
Systemsteuerung	Zugriff nur für Administratoren
Windows Update	Updates nur manuell durch Administrator
Passwort-Richtlinie	Mindestlänge, Komplexität und Ablauf
USB-Speicher	Schreibzugriff deaktivieren

5. Schritt-für-Schritt Anleitung

5.1 Schritt 1 – Desktop-Hintergrund festlegen

1. Öffnen Sie den Gruppenrichtlinien-Editor:

```
gpedit.msc
```

2. Navigieren Sie zu:

```
Benutzerkonfiguration  
→ Administrative Vorlagen  
→ Desktop  
→ Desktop
```

3. Öffnen Sie die Richtlinie:

```
Desktop-Hintergrund
```

4. Aktivieren Sie die Richtlinie und geben Sie den Pfad zum Firmenlogo an, z. B.:

```
C:\Firmenlogo\logo.jpg
```

5. Setzen Sie die Richtlinie auf **Aktiviert**, damit der Hintergrund nicht geändert werden kann.

5.2 Schritt 2 – Zugriff auf Systemsteuerung einschränken

1. Navigieren Sie zu:

Benutzerkonfiguration

→ Administrative Vorlagen

→ Systemsteuerung

2. Öffnen Sie die Richtlinie:

Zugriff auf Systemsteuerung und PC-Einstellungen verweigern

3. Aktivieren Sie die Richtlinie.

Damit wird verhindert, dass normale Benutzer die Systemsteuerung öffnen können.

5.3 Schritt 3 – Windows Update nur manuell

1. Navigieren Sie zu:

Benutzerkonfiguration

→ Administrative Vorlagen

→ Windows-Komponenten

→ Windows Update

2. Öffnen Sie die Richtlinie:

Automatische Updates konfigurieren

3. Stellen Sie folgende Option ein:

2 – Vor Download und Installation benachrichtigen

Damit können Updates nur durch Administratoren gestartet werden.

5.4 Schritt 4 – Passwort-Richtlinie konfigurieren

Navigieren Sie zu:

Computerkonfiguration

- Windows-Einstellungen
- Sicherheitseinstellungen
- Kontorichtlinien
- Kennwortrichtlinie

Konfigurieren Sie folgende Einstellungen:

Minimale Kennwortlänge

10 Zeichen

Kennwort muss Komplexitätsanforderungen erfüllen

Aktiviert

Maximales Kennwortalter

90 Tage

Diese Einstellungen erhöhen die Sicherheit der Benutzerkonten.

5.5 Schritt 5 – USB-Schreibzugriff deaktivieren

Navigieren Sie zu:

Computerkonfiguration

- Administrative Vorlagen
- System
- Wechselmedienzugriff

Öffnen Sie die Richtlinie:

Wechselmedien: Schreibzugriff verweigern

Setzen Sie die Richtlinie auf:

Aktiviert

Damit können USB-Sticks nur noch gelesen, aber nicht mehr beschrieben werden.

6. Ergebnis / Kontrolle

Nach der Implementierung gelten folgende Einschränkungen:

- Desktop-Hintergrund mit Firmenlogo ist festgelegt
- Normale Benutzer haben keinen Zugriff auf die Systemsteuerung
- Windows Updates können nur durch Administratoren gestartet werden
- Passwörter müssen mindestens 10 Zeichen lang sein und komplex sein
- USB-Sticks erlauben nur Lesezugriff

Zur Überprüfung kann folgender Befehl verwendet werden:

```
gpresult /h gpo-report.html
```

Dieser erstellt einen Bericht über alle angewendeten Gruppenrichtlinien.

7. Dokumentation / Abgabe

Für die Abgabe sollten folgende Nachweise enthalten sein:

- Screenshots der GPO-Einstellungen
- Screenshot des Gruppenrichtlinien-Editors
- generierter Bericht

```
gpo-report.html
```

kurze Beschreibung der implementierten Richtlinien

8. Anhang (optional)

Optional können ergänzt werden:

- Screenshots aller Richtlinien
- Test mit einem normalen Benutzerkonto
- Screenshot des Desktop-Hintergrunds mit Firmenlogo