

HowTo – NTFS-Berechtigungen

Kategorie	[z.B. Windows Administration]
Autor	Lugstein Markus
Datum	
Version	1.0

Inhalt

1. Ziel der Anleitung	2
2. Voraussetzungen.....	2
3. Warnhinweise	2
4. Übersicht der Aufgabe	2
5. Schritt-für-Schritt Anleitung	3
5.1 Schritt 1 – Vererbung entfernen und Berechtigungen zurücksetzen	3
5.2 Schritt 2 – Administratoren Vollzugriff geben	3
5.3 Schritt 3 – Fachgruppen mit Änderungsrechten	3
5.4 Schritt 4 – Share-Ordner nur Lesen.....	4
5.5 Schritt 5 – Entfernen von Domain Users.....	4
6. Ergebnis / Kontrolle	4
Berechtigungen prüfen mit:.....	4
7. Dokumentation / Abgabe	4
8. Anhang	5
8.1 Wichtige NTFS-Berechtigungen im Überblick	5
8.2 Vererbungs-Flags (wichtig für Ordner).....	5
8.3 Typische Kombinationen (Praxis)	5
9. Beispiel: Samba-/SMB-Share per PowerShell erstellen	6
9.1 Samba-/SMB-Share per PowerShell erstellen.....	6
9.2 Kontrolle	6

1. Ziel der Anleitung

Ziel ist es, für die Ordnerstruktur unter C:\Daten klare und sichere NTFS-Berechtigungen zu setzen:

- Fachgruppen erhalten Zugriff nur auf ihren Bereich
- Gemeinsamer Ordner (share) ist nur lesbar
- Andere Benutzer haben keinen Zugriff
- Administratoren behalten volle Kontrolle

2. Voraussetzungen

- PowerShell oder CMD mit Administratorrechten
- Vorhandene AD-Gruppen:
 - GG_IT
 - GG_Vertrieb
 - GG_Verwaltung
- Ordnerstruktur:
 - C:\Daten\IT
 - C:\Daten\Vertrieb
 - C:\Daten\Verwaltung
 - C:\Daten\share

3. Warnhinweise

- ⚠ /reset entfernt bestehende Berechtigungen
- ⚠ Falsche Anwendung kann Zugriff komplett sperren
- ⚠ Immer sicherstellen, dass Administratoren Zugriff behalten
- ⚠ Test idealerweise zuerst in einer Testumgebung

4. Übersicht der Aufgabe

Für jeden Ordner werden:

- Vererbung deaktiviert
- Alte Berechtigungen entfernt
- Neue Berechtigungen gezielt gesetzt

5. Schritt-für-Schritt Anleitung

5.1 Schritt 1 – Vererbung entfernen und Berechtigungen zurücksetzen

Für jeden Ordner ausführen:

```
icaccls "C:\Daten\IT" /inheritance:r  
icaccls "C:\Daten\IT" /reset  
  
icaccls "C:\Daten\Vertrieb" /inheritance:r  
icaccls "C:\Daten\Vertrieb" /reset  
  
icaccls "C:\Daten\Verwaltung" /inheritance:r  
icaccls "C:\Daten\Verwaltung" /reset  
  
icaccls "C:\Daten\share" /inheritance:r  
icaccls "C:\Daten\share" /reset
```

5.2 Schritt 2 – Administratoren Vollzugriff geben

```
icaccls "C:\Daten\IT" /grant "Administratoren:(OI)(CI)F"  
icaccls "C:\Daten\Vertrieb" /grant "Administratoren:(OI)(CI)F"  
icaccls "C:\Daten\Verwaltung" /grant "Administratoren:(OI)(CI)F"  
icaccls "C:\Daten\share" /grant "Administratoren:(OI)(CI)F"
```

5.3 Schritt 3 – Fachgruppen mit Änderungsrechten

```
icaccls "C:\Daten\IT" /grant "DOMAIN\GG_IT:(OI)(CI)M"  
icaccls "C:\Daten\Vertrieb" /grant "DOMAIN\GG_Vertrieb:(OI)(CI)M"  
icaccls "C:\Daten\Verwaltung" /grant "DOMAIN\GG_Verwaltung:(OI)(CI)M"
```

5.4 Schritt 4 – Share-Ordner nur Lesen

```
icacls "C:\Daten\share" /grant "DOMAIN\GG_IT:(OI)(CI)RX"  
icacls "C:\Daten\share" /grant "DOMAIN\GG_Vertrieb:(OI)(CI)RX"  
icacls "C:\Daten\share" /grant "DOMAIN\GG_Verwaltung:(OI)(CI)RX"
```

5.5 Schritt 5 – Entfernen von Domain Users

```
icacls "C:\Daten\IT" /remove "DOMAIN\Domain Users"  
icacls "C:\Daten\Vertrieb" /remove "DOMAIN\Domain Users"  
icacls "C:\Daten\Verwaltung" /remove "DOMAIN\Domain Users"  
icacls "C:\Daten\share" /remove "DOMAIN\Domain Users"
```

6. Ergebnis / Kontrolle

Berechtigungen prüfen mit:

```
icacls "C:\Daten\IT"
```

Erwartetes Ergebnis:

- Nur passende GG-Gruppe hat Zugriff
- Administratoren haben Vollzugriff
- Keine „Domain Users“ mehr vorhanden

7. Dokumentation / Abgabe

- Durchgeführte Befehle dokumentieren
- Screenshot der gesetzten Berechtigungen
- ggf. Export:

```
icacls "C:\Daten" /save C:\temp\rechte.txt /T
```

8. Anhang

8.1 Wichtige NTFS-Berechtigungen im Überblick

Kürzel	Name (engl.)	Name (deutsch)	Beschreibung
F	FullControl	Vollzugriff 	Alles erlaubt inkl. Berechtigungen ändern
M	Modify	Ändern 	Lesen, Schreiben, Löschen
RX	Read & Execute	Lesen & Ausführen 	Dateien lesen + Programme ausführen
R	Read	Lesen 	Nur lesen
W	Write	Schreiben 	Dateien erstellen/ändern
D	Delete	Löschen 	Dateien löschen

8.2 Vererbungs-Flags (wichtig für Ordner)

Kürzel	Bedeutung	Erklärung
(OI)	Object Inherit	Gilt für Dateien 
(CI)	Container Inherit	Gilt für Unterordner 
(IO)	Inherit Only	Nur vererbt, nicht direkt auf Ordner
(NP)	No Propagate	Nicht weitervererben

8.3 Typische Kombinationen (Praxis)

Kombination	Bedeutung
(OI)(CI)F	Vollzugriff auf alles darunter
(OI)(CI)M	Ändern auf Ordner + Inhalt
(OI)(CI)RX	Nur Lesen auf alles
(CI)(IO)M	Nur Unterordner bekommen Modify
(OI)(IO)R	Nur Dateien bekommen Leserechte

9. Beispiel: Samba-/SMB-Share per PowerShell erstellen

neuen Ordner „Test“ unter C:\Daten\ erstellen

```
New-Item -Name "Test" -ItemType Directory
```

9.1 Samba-/SMB-Share per PowerShell erstellen

```
$folder = "C:\Daten\Test"
$shareName = "Test"
$group = "DOMAIN\GG_Verwaltung"

# SMB-Share erstellen
New-SmbShare `
  -Name $shareName `
  -Path $folder `
  -FullAccess "Administratoren" `
  -ChangeAccess $group
```

Was passiert hier?

- New-SmbShare → erstellt die Windows-Freigabe (SMB = „Windows-Samba“)
- -Name Verwaltung → so erscheint der Share im Netzwerk
- -Path → Zielordner
- -FullAccess Administratoren → Admins haben Vollzugriff 🏰
- -ChangeAccess GG_Verwaltung → Gruppe darf lesen + schreiben

Ganz wichtig (der Klassiker!)

SMB-Share-Rechte allein reichen nicht!

👉 NTFS-Berechtigungen müssen auch passen (sonst: Zugriff verweigert 🙄)

Falls noch nicht gesetzt:

```
icacls "C:\Daten\Test" /grant "DOMAIN\GG_Verwaltung:(OI)(CI)M"
icacls "C:\Daten\Test" /grant "Administratoren:(OI)(CI)F"
```

9.2 Kontrolle

```
Get-SmbShare -Name Test
Get-SmbShareAccess -Name Test
```