



# NEXT GEN

---

ENDLICH KONTROLLE ÜBER IHRE  
KOMPLEXEN MICROSOFT-BERECHTIGUNGEN

---

**Berechtigungen im AD, NTFS Filesystem, Exchange,  
Sharepoint, Entra ID & Co. übersichtlich darstellen  
und Missstände automatisiert erkennen**

**René Leitz, Product Manager daccord**

# Vorbemerkungen

Wer kennt es nicht, dieses sorgenvolle Gefühl, wenn es um Berechtigungsvergaben im Active Directory und um Zugriffsrechte auf Dateiservern geht?

Je größer die Umgebung wird, desto unübersichtlicher kann es schnell werden.

Wie schnell könnten beispielsweise unerlaubte Zugriffe über verwaiste Konten zu schwerwiegenden Folgen führen? Hier den Überblick zu behalten und wirklich sicher zu sein, ist mit Bordmitteln oftmals eine große Herausforderung.

[ZUM ERKLÄRVIDEO](#)



# Berechtigungen in Microsoft-Umgebungen

- Ein Frontend zur Analyse aller Microsoft Berechtigungen
- Durch „Integrationspakete“ wie z.B. Active Directory, MS Fileserver, Entra ID, Exchange erweiterbar
- Sofortige Erkennung von Missständen durch mitgelieferte „Richtlinien“
- Historische Speicherung aller Veränderungen
- Spezielle „Effektive-Rechte-Sichtweisen“ zur Beantwortung der Frage: Was darf Max Mustermann?

# Was sind Richtlinien?

- Vorgefertigte Analysen Ihrer Daten wie z.B.
  - gibt es im Active Directory mit sich selbst verschachtelte Gruppen
  - gibt es ausgeschiedene Mitarbeiter mit noch aktiven Benutzerkonten
- Schwachstellen werden direkt nach der Installation angezeigt
- Beurteilung der Daten auf Basis von Schwellenwerten und Einstufung des Missstandes in verschiedene Risikolevel
- Zeitgesteuerte Ausführung um einen historischen Verlauf abzubilden (Verbesserung oder Verschlechterung)
- Individuelle Richtlinien nach Kundenanforderung möglich

# Anwendungsfälle

Anwendungsfall 1:

Was darf Peter Walk?

Anwendungsfall 2:

Richtlinienverstoß im MS Fileserver

Anwendungsfall 3:

Gibt es fehlerhafte Gruppenverschachtelungen (Loops) im Active Directory?

Anwendungsfall 4:

Gab es Änderungen in der Domain Admin-Gruppe im Active Directory?



# Anzeige aller Benutzerkonten einer Person

daccord Home **Personen** Active Directory Fileserver Entra ID Exchange

## Personen

Alle Personen

Nachname	Vorname	Firma	Organisationseinheit	Standort
walk	peter			

Anzahl: 20 von 1

Nachname	Vorname	Firma	Organisationseinheit
Walk	Peter	daccord	Planning

### Peter Walk

Personal-Nr. 100022

Vorname Peter

Nachname Walk

Status  Aktiv

Typ Interner Mitarbeiter

### Konten

- Active Directory (DACCORD) - PWalk ✓
- Fileserver (DACCORD) - PWalk ✓
- Exchange (EXCHANGE) - PWalk@daccord.de
- Entra ID (daccord.de) - Peter Walk ✓

### Organisation

### Kontakt

# MS Fileserver Berechtigungen

## Fileserver (DACCORD) ...



✓ Aktiver Person zugewiesen

DN CN=Peter Walk,OU=User\_Standard\_intern,OU=Headquarter,OU=Organisation,DC=daccord,DC=de

sAMAccountName PWalk

Vorname Peter

Name Walk

Status ✓ Aktiv

mehr Informationen ▲

Gruppen ▲

Effektive Rechte

### Zugriffsberechtigungen auf Verzeichnisse und Dateien

- Connector
- Consulting
- Contracts
- Engineering
- Geschäftsleitung
- Human Resources
- IT
- Marketing
- Planning
- Azubiprojekte
- CAD Software
- Planung
- Shared
- Teamlead**
- Technisches

## Teamlead



Kompletter Pfad \\GUHTESTSRV001\C\$\DATADRIVE\p. #

Vererbung aktiv

Besitzer Administratoren

Effektiv

Erhalten über

Ordner Berechtigungen

Die angezeigten effektiven Rechte beziehen sich auf den ausgewählten User .

- ✗ Vollzugriff
- ✓ Ordner durchsuchen / Datei ausführen
- ✓ Ordner auflisten / Daten lesen
- ✓ Attribute lesen
- ✓ Erweiterte Attribute lesen
- ✓ Dateien erstellen / Daten schreiben
- ✓ Ordner erstellen / Daten anhängen
- ✓ Attribute schreiben
- ✓ Erweiterte Attribute schreiben
- ✗ Unterordner und Dateien löschen
- ✓ Löschen
- ✓ Berechtigungen lesen
- ✗ Berechtigungen ändern
- ✗ Besitz übernehmen

# MS Fileserver Berechtigungen

## Fileserver (DACCORD) ...



✓ Aktiver Person zugewiesen

DN	CN=Peter Walk,OU=User_Standard_intern,OU=Headquarter,OU=Organisation,DC=daccord,DC=de
sAMAccountName	PWalk
Vorname	Peter
Name	Walk
Status	✓ Aktiv

mehr Informationen ▲

Gruppen ▲

Effektive Rechte

### Zugriffsberechtigungen auf Verzeichnisse und Dateien

- Connector
- Consulting
- Contracts
- Engineering
- Geschäftsleitung
- Human Resources
- IT
- Marketing
- Planning
- Azubiprojekte
- CAD Software
- Planung
- Shared
- Teamlead**
- Technisches

## Teamlead



Kompletter Pfad	\\GUHTESTSRV001\C\$\DATADRIVE\P. #
Vererbung	aktiv
Besitzer	Administratoren

Effektiv Erhalten über Ordner Berechtigungen

Die angezeigte Analyse der Rechte bezieht sich auf den ausgewählten User .

### Share

	Vererbung	Vollzugriff	Ändern	Lesen
Everyone	§	✓	✓	✓

### NTFS

	Vererbung	Vollzugriff	Ändern	Lesen, Ausführen	Lesen	Schreiben	Spezielle Rechte
L_Planning_Teamlead_RW	§			✓	✓		
L_Planning_RO	↓		✓	✓	✓	✓	

# MS Exchange Berechtigungen

## Exchange (EXCHANGE) -...

✓ Aktiver Person zugewiesen

Mailbox ID	PWalk@daccord.de
sAMAccountName	PWalk
Name	PWalk@daccord.de
Anzeigename	Peter Walk
Besitzer	PWalk
Exchange System	EXCHANGE
Kategorie	UserMailbox
Datenbank	DB1

### E-Mail Adressen

### Weitere Attribute

### Berechtigungen

	Vollzugriff	Ändern	Berechtigungen lesen	Senden als	Senden im Auftrag von	Sonst. Berechtigungen
👤 CJuanez	✓				✓	
👤 CRocker	✓				✓	
👤 PWalk	✓		✓			

### Mailbox Berechtigungen

### Zugriffsberechtigungen auf Mailboxen

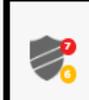
	Vollzugriff	Besitzer ändern	Berechtigungen ändern	Berechtigungen lesen	Senden als	Senden im Auftrag von	Sonst. Berechtigungen
✉ PWalk@daccord.de	✓			✓			
✉ PKinzinger@daccord.de	✓					✓	
✉ Planung@daccord.de	✓				✓		
✉ AYariz@daccord.de					✓		
✉ hgverkn@daccord.de	✓						



# MS Fileserver: Hinweis zum Richtlinienverstoß

**daccord** Home Personen Active Directory **Fileserver** Entra ID Exchange admin, daccord DE

## Fileserver

Alle Fileserver  3 

 **3** verschiedene Fileserver

 **295** Ordner auf dem Fileserver

 **4** lokale User auf dem Fileserver

 **25** lokale Gruppen auf dem Fileserver

Fileserver User und Gruppen Shares, Ordner und Dateien

Alle   

Name
 GUHTESTSRV002
 GUHTESTSRV001
 GUHTESTEX001

# MS Fileserver: Kritische Richtlinien

daccord Home Personen Active Directory **Fileserver** Entra ID Exchange admin, daccord DE ?

Fileserver 3 2

Alle Fileserver

☰

**7** kritische Richtlinien anzeigen

**6** weniger kritische Richtlinien anzeigen

**20** alle Richtlinien anzeigen

**Datenbereiche mit unterbrochener Vererbung** - Es gibt 62 Ordner bei denen die Vererbung unterbrochen ist.

**Benutzerkonten mit Vollzugriff** - Es gibt 11 Benutzerkonten mit Vollzugriffs-Berechtigungen.

**Andere Besitzer als "Administratoren" oder "System"** - Es gibt 127 Ordner oder Dateien mit anderen Besitzern als die Gruppe "Administrators" oder "System".

**Berechtigungen für "Jeder"** - Es gibt 12 Ordnern, Dateien oder Freigaben auf welche die Gruppe "Jeder" Berechtigungen besitzt.

**Benutzerkonten mit direkten Berechtigungen** - Es gibt 12 Benutzerkonten mit direkten Berechtigungszuweisungen zu Ordnern oder Dateien.

**Ordner der 2. Ebene mit direkt vergebenen Userberechtigungen** - Es gibt 13 Ordner der 2. Ebene mit direktem Userzugriff

**Ordner der 1. Ebene ohne System- oder Administratorenzugriff** - Es gibt 4 Ordner ohne System- oder Administratorenzugriff

# MS Fileserver: Richtlinien-Auswertung

## Benutzerkonten mit direkten Berechtigungen

**Beschreibung:**  
Nach den Empfehlungen von Microsoft (AGDLP Konzept) sollten Benutzerkonten möglichst keine direkt vergeben Berechtigungen besitzen.

**Auswertungsdetails:**  
Die Auswertungen haben ergeben, dass Benutzerkonten existieren, die direkt vergebene Berechtigungen auf Ordner oder Dateien besitzen.

**Empfehlung:**  
Weisen Sie (nach dem empfohlenen ADGLP Prinzip) die Benutzerkonten den globalen Gruppen zu, die wiederum Mitglied der domänenlokalen Gruppen werden. Vergeben Sie dann die Berechtigungen in den domänenlokalen Gruppen. Weitere Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) bezüglich Fileserver finden Sie im IT Grundschutz Kompendium unter Artikel APP.3.3 Fileserver oder unter Artikel SYS.1.2.2 Windows Server. Hier erhalten Sie Empfehlungen des BSI zum Thema "Absicherung von Windows Server 2012 und Windows Server 2012 R2".

Es gibt 12 Benutzerkonten mit direkten Berechtigungszuweisungen zu Ordnern oder Dateien.

System	Benutzername	ID	Nachname	Vorname	Zuletzt benutzt	Anzahl Ordner	Anzahl Dateien	Status
DACCORD	power	CN=power test,OU=Servicekonten,OU=G&H,OU=Organisation,DC=daccord,DC=de	test	power	24.12.2021	2	0	✓
DACCORD	hgueltig	CN=Harald\, Gültig / Test,OU=G&H,OU=Organisation,DC=daccord,DC=de	Gültig Sonderzeichen: §	Harald	01.01.1601	1	0	✓
DACCORD	daccord-admin	CN=daccord- admin,OU=IT,OU=G&H,OU=Organisation,DC=daccord,DC=de		daccord-admin	08.10.2023	20	0	✓
DACCORD	mbloch	CN=Matthias Bloch,OU=IT,OU=G&H,OU=Organisation,DC=daccord,DC=de	Bloch	Matthias	17.08.2022	2	0	✓
DACCORD	GSchmidtmeier	CN=Gisela Schmidtmeier,OU=User_Standard_Intern,OU=Headquarter,OU=Organisa	Schmidtmeier	Gisela	01.01.1601	1	0	✓

# MS Fileserver: Richtlinien-Auswertung

**daccord** Home Personen Active Directory **Fileserver** Entra ID Exchange

## Benutzerkonten mit direkten Berechtigungen

**Beschreibung:**  
Nach den Empfehlungen von Microsoft (AGDLP Konzept) sollten Benutzerkonten möglichst keine direkt vergebene Berechtigungen besitzen.

**Auswertungsdetails:**  
Die Auswertungen haben ergeben, dass Benutzerkonten existieren, die direkt vergebene Berechtigungen auf Ordner oder Dateien besitzen.

**Empfehlung:**  
Weisen Sie (nach dem empfohlenen ADGLP Prinzip) die Benutzerkonten den globalen Gruppen zu, die wiederum Mitglied der domänenlokalen Gruppen werden. Vergeben Sie dann die Berechtigungen für Sicherheit in der Informationstechnologie (BSI) bezüglich Fileserver finden Sie im IT Grundschatz Kompendium unter Artikel APP.3.3 Fileserver oder unter Artikel SYS.1.2.2 Windows Server. Hi Server 2012 und Windows Server 2012 R2".

**Es gibt 12 Benutzerkonten mit direkten Berechtigungszuweisungen zu Ordnern oder Dateien.**

ZURÜCK ZUR ÜBERSICHT Benutzerkonto: GSCHMIDTMEIER

System	Typ	Name	ID
GUHTESTSRV001	📁	Budgets	\\GUHTESTSRV001\C\$\DATADRIVE\Geschäftsleitung\Finanzen\Budgets

## Budgets

Kompletter Pfad 📄 \\GUHTESTSRV001\C\$\DATADRIVE\G #

Vererbung aktiv

Besitzer 👤 Administratoren

### NTFS

	Vererbung	Vollzugriff	Ändern	Lesen, Ausführen	Lesen	Schreiben	Spezielle Rechte
👤 Administratoren	📄	✅	✅	✅	✅	✅	▶
👤 Benutzer	📄						✅
👤 Benutzer	📄			✅	✅		
👤 Domänen-Admins	📄			✅	✅		
👤 L_Geschaeftsleitung_Finanz...	📄			✅	✅		
👤 L_Geschaeftsleitung_RO	📄		✅	✅	✅	✅	
👤 System	📄	✅	✅	✅	✅	✅	
👤 GSchmidtmeier	📄	✅	✅	✅	✅	✅	

# Historischer Verlauf

## Benutzerkonten mit direkten Berechtigungen

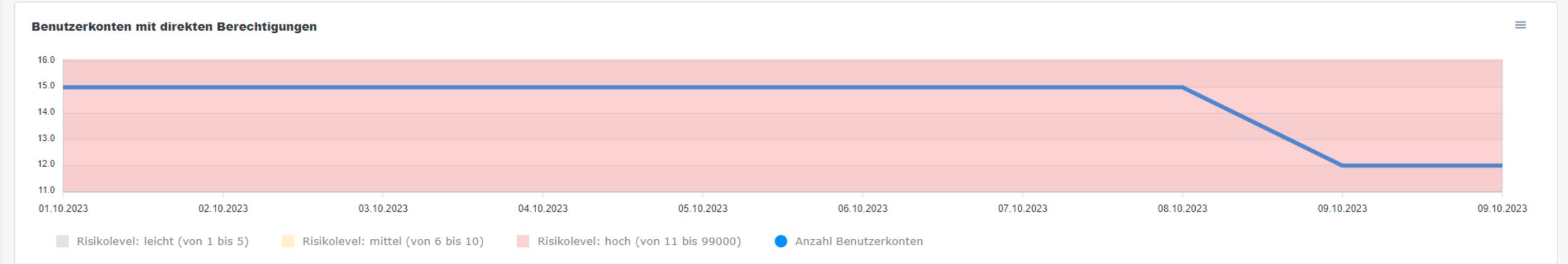
**Beschreibung:**  
Nach den Empfehlungen von Microsoft (AGDLP Konzept) sollten Benutzerkonten möglichst keine direkt vergeben Berechtigungen besitzen.

**Auswertungsdetails:**  
Die Auswertungen haben ergeben, dass Benutzerkonten existieren, die direkt vergebene Berechtigungen auf Ordner oder Dateien besitzen.

**Empfehlung:**  
Weisen Sie (nach dem empfohlenen ADGLP Prinzip) die Benutzerkonten den globalen Gruppen zu, die wiederum Mitglied der domänenlokalen Gruppen werden. Vergeben Sie dann die Berechtigungen in den domänenlokalen Gruppen. Weitere Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) bezüglich Fileserver finden Sie im IT Grundschatz Kompendium unter Artikel APP.3.3 Fileserver oder unter Artikel SYS.1.2.2 Windows Server. Hier erhalten Sie Empfehlungen des BSI zum Thema "Absicherung von Windows Server 2012 und Windows Server 2012 R2".

Es gibt 12 Benutzerkonten mit direkten Berechtigungszuweisungen zu Ordnern oder Dateien.

Historie anzeigen für:



---

ANWENDUNGSFALL 3:

GIBT ES FEHLERHAFTE  
GRUPPENVERSCHACHTELUNGEN  
(LOOPS) IM ACTIVE DIRECTORY?

---

# Fehlerhafte Gruppenverschachtelungen (Loops)

 daccord Home Personen **Active Directory** Fileserver Exchange Entra ID Administrator, Portal  DE  

Active Directory  1 

Alle User & Gruppen 

**3** kritische Richtlinien anzeigen

**0** weniger kritische Richtlinien anzeigen

**4** alle Richtlinien anzeigen

**Mit sich selbst verschachtelte Gruppen** - Es gibt 3 Gruppen die mit sich selbst verschachtelt sind.

**Domänenlokale Gruppen mit Benutzerkonten** - Es gibt 5 Domänen-lokale Gruppen mit Benutzerkonten als Mitglieder.

**Große Anzahl an Domänen-Admins** - Es gibt 12 Benutzerkonten mit Mitgliedschaft in der Gruppe: Domänen-Admins.

**Zu viele Gruppenmitgliedschaften** - Es gibt 0 Benutzerkonten, bei denen die maximale Anzahl (max. 1015) an Gruppenmitgliedschaften überschritten oder erreicht ist.

# Fehlerhafte Gruppenverschachtelungen (Loops)

## Mit sich selbst verschachtelte Gruppen

### Beschreibung:

Active Directory Gruppen, welche mit sich selbst verschachtelt sind, können innerhalb von Anwendungen oder Skripten zu Problemen in Form von Abstürzen, unendlichen Schleifen und ungewollten Fehlermeldungen führen. Zirkuläre Verschachtelungen sind aus diesem Grund möglichst zu vermeiden.

### Auswertungsdetails:

Im Active Directory System gibt es Gruppen, die mit sich selbst verschachtelt sind.

### Empfehlung:

Überprüfen Sie Ihre Gruppenkonstellation und beheben Sie die zirkuläre Verschachtelung.

Es gibt 3 Gruppen die mit sich selbst verschachtelt sind.



Gruppenname	ID	Domain	Scope	Kategorie	Anzahl Verschachtelung
ROL_Purchasing-Employees	CN=ROL_Purchasing-Employees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_Trainees	CN=ROL_Trainees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_TEMP	CN=ROL_TEMP,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1

# Fehlerhafte Gruppenverschachtelungen (Loops)

## Mit sich selbst verschachtelte Gruppen

### Beschreibung:

Active Directory Gruppen, welche mit sich selbst verschachtelt sind, können innerhalb von Anwendungen oder Skripten zu Problemen in Form von Abstürzen, unendlichen Schleifen und ungewollten Fehlermeldungen führen. Zirkuläre Verschachtelungen sind aus diesem Grund möglichst zu vermeiden.

### Auswertungsdetails:

Im Active Directory System gibt es Gruppen, die mit sich selbst verschachtelt sind.

### Empfehlung:

Überprüfen Sie Ihre Gruppenkonstellation und beheben Sie die zirkuläre Verschachtelung.

Es gibt 3 Gruppen die mit sich selbst verschachtelt sind.



[← ZURÜCK ZUR ÜBERSICHT](#)

Gruppe: ROL\_PURCHASING-EMPLOYEES

Gruppenname	ID	Domain	Scope	Kategorie	Reihenfolge
ROL_TEMP	CN=ROL_TEMP,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_Trainees	CN=ROL_Trainees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_Purchasing-Employees	CN=ROL_Purchasing-Employees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	2

# Fehlerhafte Gruppenverschachtelungen (Loops)

**daccord** Home Personen **Active Directory** Fileserver Exchange Entra ID Administrator, Portal DE

Active Directory 1 3

Alle User & Gruppen

**DACCORD** **99** User im Active Directory **296** Gruppen im Active Directory

System: DACCORD Name der Gruppen: Spezial Filter: Gruppen mit Selbstverschachtelung Anzeige Ebenen: 1 Ebenen Limit: 25

Historie:

```
graph TD; ROL_TEMP((ROL_TEMP)) --> ROL_Purchasing-Employees((ROL_Purchasing-Employees)); ROL_Purchasing-Employees --> ROL_Trainees((ROL_Trainees)); ROL_Trainees --> ROL_TEMP;
```

**daccord**



## ANWENDUNGSFALL 4:

GAB ES ÄNDERUNGEN IN DER DOMAIN  
ADMIN GRUPPE IM ACTIVE DIRECTORY?



# Gruppe Domänen-Admins

**daccord** Home Personen **Active Directory** Fileserver Entra ID Exchange

## Active Directory

Alle User & Gruppen

 **DACCORD**

 **99** User im Active Directory

 **329** Gruppen im Active Directory

Active Directory	Name	Beschreibung	Kategorie
DACCORD	domän		Alle

Anzahl: 10 von 5

Name	Beschreibung	Domain
Domänen-Admins	Administratoren der Domäne	DACCOR
Domänen-Benutzer	Alle Domänenbenutzer	DACCOR
Domänen-Gäste	Alle Domänengäste	DACCOR
Domänencomputer	Alle Arbeitsstationen und Computer der Domäne	DACCOR
Domänencontroller	Alle Domänencontroller der Domäne	DACCOR

### Domänen-Admins

ObjectSid: S-1-5-21-1104076897-471672909-1837833638-512

DN: CN=Domänen-Admins,CN=Users,DC=daccord,DC=de

Domain: DACCORD

CN: Domänen-Admins

Beschreibung: Administratoren der Domäne

Erstellt am: 13.01.2021

Geändert am: 09.10.2023

Kategorie: Sicherheitsgruppen

Scope: Global

#### Mitglieder

- daccord-admin
- mbloch
- sspethmann
- dmse\_service
- Administrator

# Gruppe Domänen-Admins Historie

**daccord** Home Personen **Active Directory** Fileserver Entra ID Exchange

## Active Directory

Alle User & Gruppen

**DACCORD** **99** User im Active Directory **329** Gruppen im Active Directory

Active Directory	Name	Beschreibung	Kategorie
DACCORD	domän		Alle

Anzahl: 10 von 5

Name	Beschreibung	Domain
Domänen-Admins	Administratoren der Domäne	DACCOR
Domänen-Benutzer	Alle Domänenbenutzer	DACCOR
Domänen-Gäste	Alle Domänengäste	DACCOR
Domänencomputer	Alle Arbeitsstationen und Computer der Domäne	DACCOR
Domänencontroller	Alle Domänencontroller der Domäne	DACCOR

### Domänen-Admins

#### Historie der Gruppe

letzten 30 Tage

Datum	Name	Veränderung
09.10.2023 10:52:09	modified	geändert

#### Historie der Gruppenmitgliedschaft

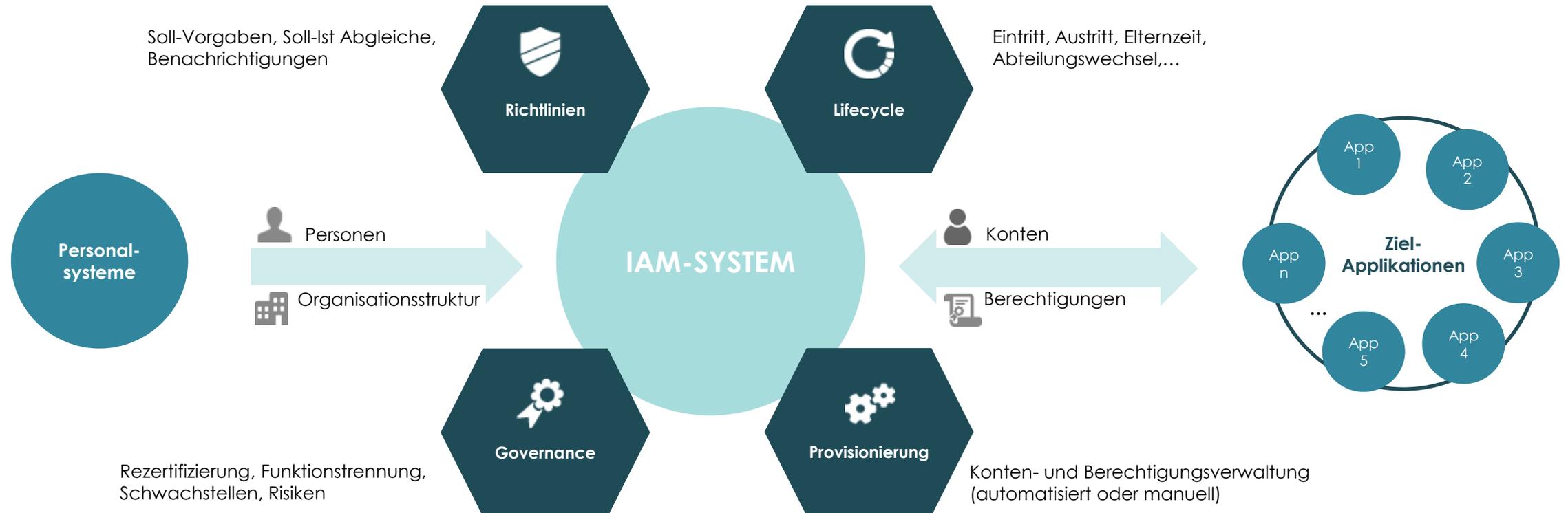
letzten 30 Tage

Datum	Mitglied	Veränderung
09.10.2023 11:00:55	PWalk	gelöscht
09.10.2023 10:56:44	PWalk	hinzugefügt
09.10.2023 10:54:12	PWalk	gelöscht
09.10.2023 10:52:12	PWalk	hinzugefügt



# daccord Next Gen

daccord Next Gen versteht sich als **DIE** zentrale Anlaufstelle für Ihr Identity & Access Management.





NEXT  
GEN

---

VIELEN DANK FÜR IHRE  
AUFMERKSAMKEIT

---

**Sie finden uns hier in Halle 7 am Stand 349!**