



it-sa 2022

Active Directory, NTFS, Exchange & Co.
Missstände automatisiert erkennen

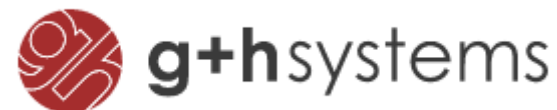
Jürgen Bähr
Geschäftsführer
j.baehr@guh-systems.de

Nürnberg, den 25. Oktober 2022

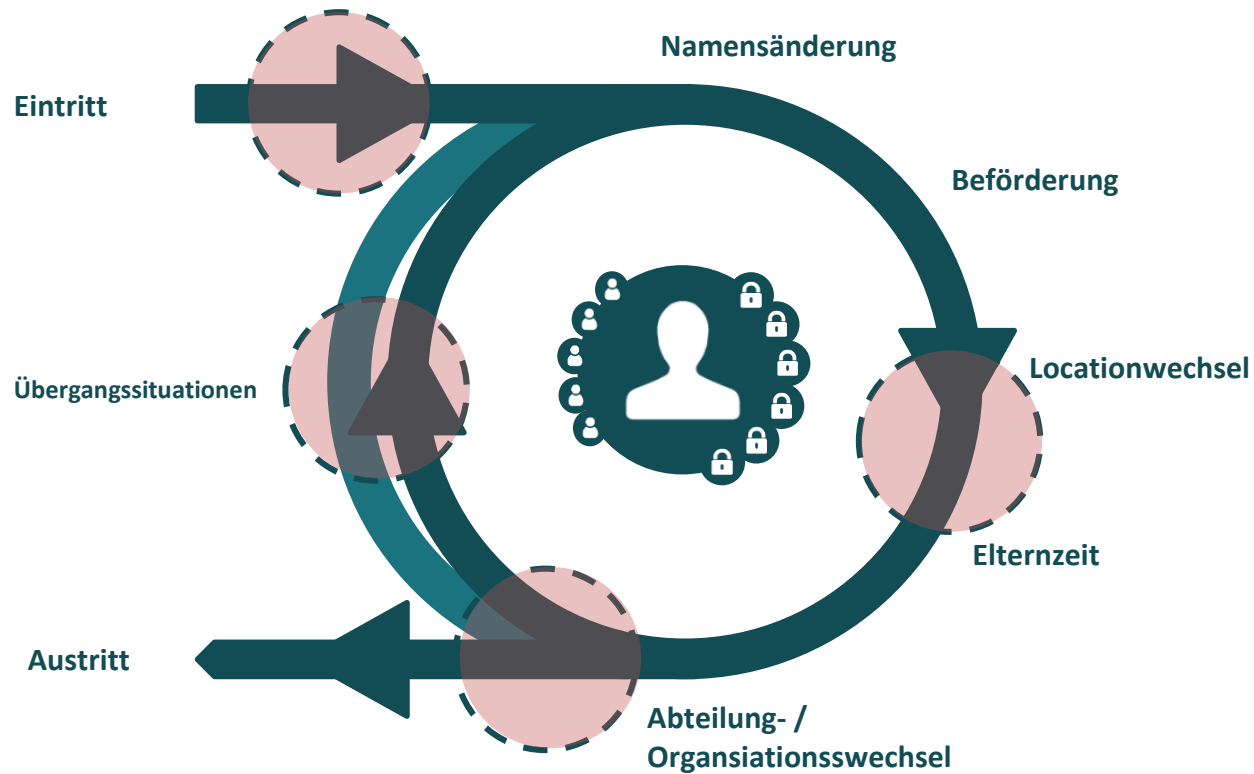
Kurzüberblick



- **G+H Systems GmbH**
- **Sitz der Gesellschaft ist Offenbach am Main**
- **Geschäftsführer**
 - Thomas Gertler
 - Jürgen Bähr
- **2005 gegründet (HRB 41799)**
- **Geschäftsfelder in DACH**
 - Consulting
 - Identity & Access Management Solutions
 - Infrastructure Solutions
 - Web- / Business Solutions
 - Produktentwicklung
 - daccord Editionen
 - inchorus
 - Service & Support



Identitäten und Berechtigungen im Wandel



Schutz der Daten in der digitalen Welt

Verband geht Verdacht auf Diebstahl von Klinik-Daten nach

Daten über Behandlungen von Patienten aus mehr als 100 Krankenhäusern in Nordrhein-Westfalen könnten illegal gestohlen worden sein.

DATENKLAU BEI VODAFONE

Der Verräter in den eigenen Reihen

Ein Insider hat bei Vodafone im großen Maßstab Daten gestohlen, zwei Millionen Kunden sind betroffen. Kein Einzelfall: Bei Wirtschaftsdelikten sitzt der Täter oft in den eigenen Reihen.

Kundendaten gestohlen? – Wenn Ex-Mitarbeiter das Vertrauen ihres Chefs missbrauchen



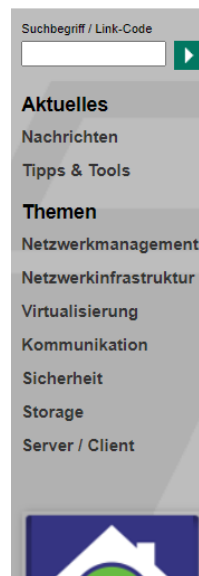
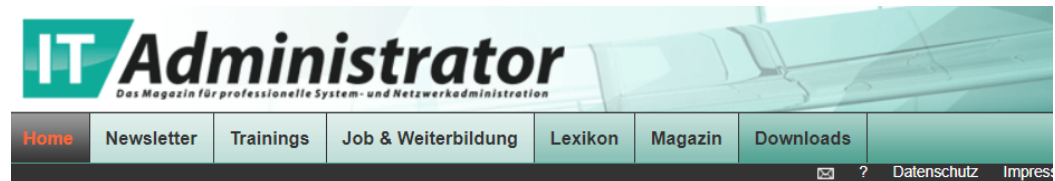
Teilen



Twittern



Teilen



Sicherheit

Fachartikel

Cyberkriminalität durch falsch gesetzte Zugriffsrechte

Nicht Wirtschaftsspione, Hacker oder gar Virenprogrammierer – die eigenen Mitarbeiter stellen in einigen Bereichen das größte Sicherheitsrisiko für Unternehmen dar. Einen wirksamen Schutz vor Betrug, Diebstahl und Korruption in den eigenen vier Wänden sehen Experten in der kontrollierten Vergabe von Zugriffsrechten.



Über einen Rechte-Drill-Down lassen sich die Berechtigungen einer Organisationseinheit nach Anwendern, Zielsystemen und Einzelrechten auflösen.

Eine aktuelle Studie der Wirtschaftsprüfungsgesellschaft KPMG unter 1001 Unternehmen aus allen Branchen gibt Anlass zur Sorge: Rund 80 Prozent der befragten Betriebe sehen ein ernstes Problem im betriebsinternen Datenklau. Bei "Verletzungen der Geschäftsgeheimnisse" gehen demnach 56 Prozent der kriminellen Machenschaften auf das Konto der eigenen Belegschaft. Die Ursachen dafür: Oftmals fehlen schlichtweg die geeigneten Instrumente, um Risikofaktoren und Compliance-Schwachstellen aufspüren zu können. Häufig mangelt es zudem an Kontrolle und Transparenz über die vergebenen Zugriffsrechte.

Unternehmenskritische Informationen landen so schnell und vor allem ohne großen Aufwand für Langfinger in den falschen Händen.

Regulatorische Vorgaben

ISO 27001 / DSGVO / MaRisk / KRITIS ..

Vermeidung unbefugter Zugriffe

Zugriffsrechte müssen kontinuierlich geprüft werden

„Need to Know“ - Prinzip

SOLL – Rollenkonzept

Rezertifizierung

daccord Editions



ACCESS GOVERNANCE EDITION #CONTROL

—
ZUGRIFFS-
BERECHTIGUNGEN
KONTROLLIEREN
—

**Globale Auswertung
und Zertifizierung
Ihrer Berechtigungen**

www.daccord.de/control



MICROSOFT EDITION #MADEFORMICROSOFT

—
BERECHTIGUNGEN
IN IHRER MICROSOFT
UMGEBUNG
—

**Analyse und Überwachung der
Berechtigungen im Active
Directory und im NTFS Filesystem**

www.daccord.de/microsoft



ADVANCED EDITION #MANAGE

—
IAM
»OUT OF THE BOX«
DAS FULL-STACK IAM
—

**Skalierbares Identity und Access
Management System inkl.
Access Governance**

www.daccord.de/manage

Konfigurationswizard



daccord

Microsoft Edition

DE



BASIS-SYSTEM

- ✓ Nutzungsbedingungen
- ✓ Datenbanken
- ✓ daccord System
- ✓ daccord Portal
- ✓ Collector Engine
- ✓ Policies Engine
- ✓ **Übersicht**



ERFOLGREICH

Ihr daccord Microsoft Edition System wurde erfolgreich konfiguriert und alle notwendigen Systemkomponenten sind bereit.

Das System kann nun von Ihnen genutzt werden.

INTEGRATIONEN

- ✓ Personendaten
- ✓ Active Directory
- ✓ Fileserver
- ✓ Exchange
- ✓ Azure Active Directory

Weiterführende Links:



Portal - Nutzen Sie zur Auswertung Ihrer Daten die personalisierten Sichtweisen im daccord Portal.



Lizenz - Erwerben oder Verlängern Sie Ihre Lizenz. Mehr dazu finden Sie an dieser Stelle.



Dokumentation - Nutzen Sie die Dokumentation, um mehr über die Verwendung der Software sowie deren Möglichkeiten und Funktionen zu erfahren.



Website - Besuchen Sie unsere offizielle Webseite und erfahren Sie mehr über die gesamte daccord Produktfamilie.

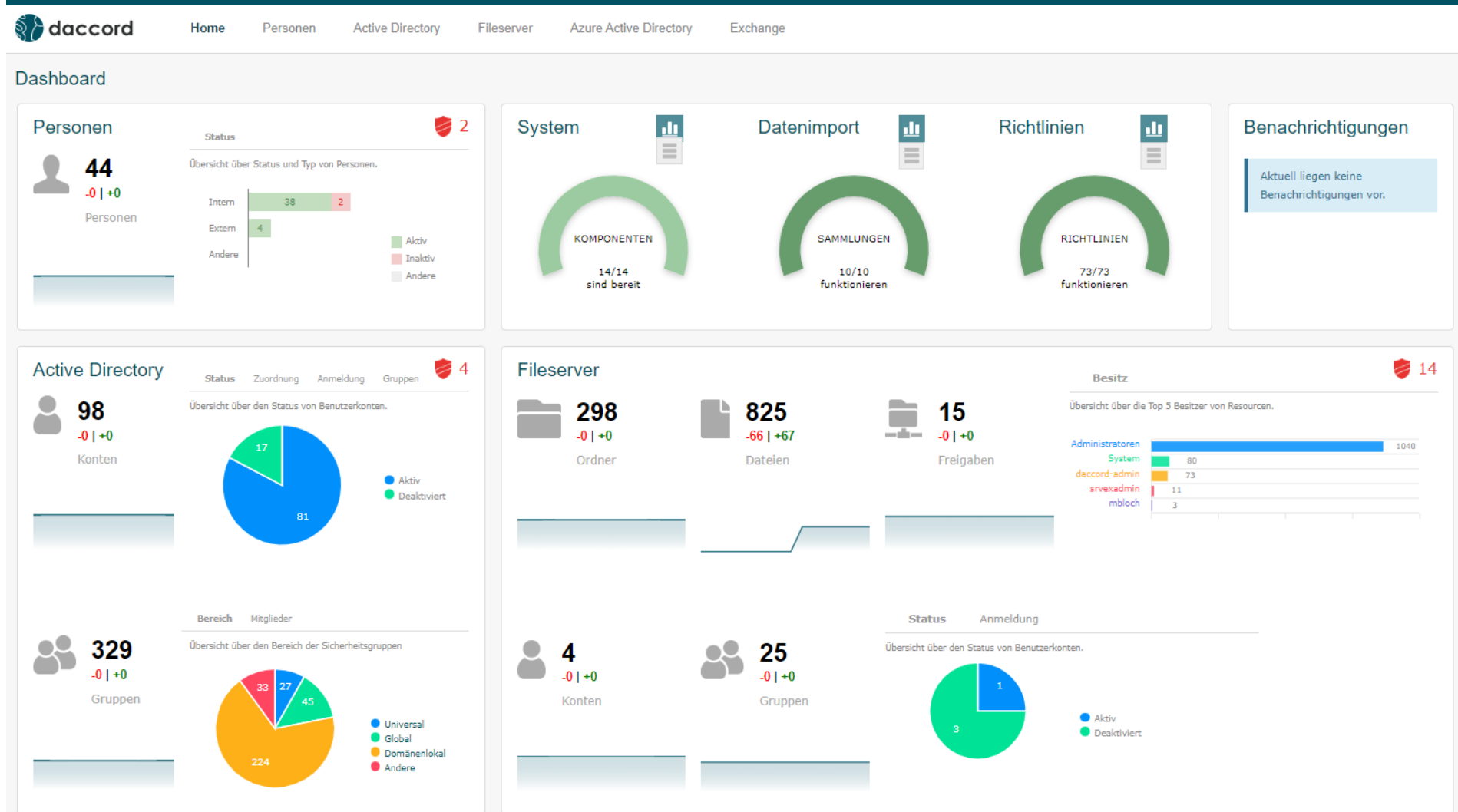


Newsletter - Bleiben Sie bezüglich der daccord Software immer auf dem neuesten Stand, indem Sie sich für unseren Newsletter registrieren.



Community - Wenn Sie Fragen oder Anregungen haben, dann nutzen Sie doch unser daccord Forum.

daccord – Microsoft Edition - DASHBOARD



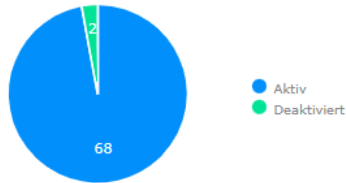
daccord – Microsoft Edition - DASHBOARD

Azure AD

 **70**
-0 | +0
Konten

Status Zuordnung Anmeldung Gruppen  4

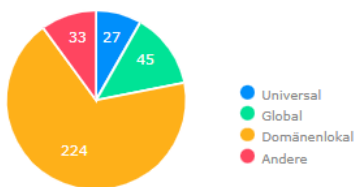
Übersicht über den Status von Benutzerkonten.



 **235**
-0 | +0
Gruppen

Bereich Mitglieder

Übersicht über den Bereich der Sicherheitsgruppen

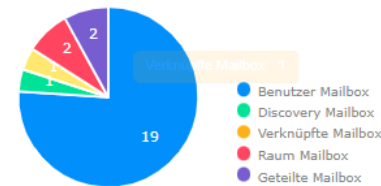


Exchange

 **25**
-0 | +25
Mailboxen

Kategorien Anmeldung Berechtigungen  2

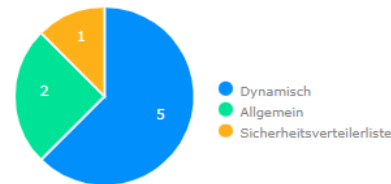
Übersicht über die Kategorien der Mailboxen



 **8**
-0 | +8
Verteilerguppen

Kategorien Mitglieder Manager

Übersicht über die Kategorien der Verteilergruppen



Benachrichtigungen

Aktuell liegen keine
Benachrichtigungen vor.

Personen - Ansichten



Home **Personen** Active Directory Fileserver Azure Active Directory Exchange

admin, daccord DE

Personen

Alle Personen

44

✓ 42
✗ 2

👤 40
👤 4

🛡️

Nachname	Vorname	Firma	Organisationseinheit	Standort	Typ	Status
					Alle	

☰

Historie: ⌚

Report: 📄

Anzahl: 20 von 44

<< < Seite 1 von 3 > >>

Nachname	Vorname	Firma	Organisationseinheit	Standort	Typ	Status
Baschtus	Viavius	daccord	Engineering	Offenbach	👤	✓
Both	Ulvi	daccord	Executive Office	Offenbach	👤	✓
Brehm	Britta	daccord	Contracting	Offenbach	👤	✓
Chang	Yen	daccord	Trainee	Offenbach	👤	✓
Clarendice	Elizabeth	daccord	Accounting	Offenbach	👤	✓
Dold	Richard	daccord	Contracting	Offenbach	👤	✓
Forster	Jannett	daccord	Planning	Offenbach	👤	✓
Ganzer	Peter	daccord	Trainee	Offenbach	👤	✓
Hahn	Reiner	daccord	Consulting	Offenbach	👤	✓
Hanselmann	Heino	daccord	Purchasing	Offenbach	👤	✓
Herzog	Aline	daccord	Accounting	Offenbach	👤	✓
Juanez	Carlos	daccord	Marketing	Offenbach	👤	✓
Kern	Julia	daccord	Sales	Offenbach	👤	✓

Personen - Ansichten



Home

Personen

Active Directory

Fileserver

Azure Active Directory

Exchange

admin, daccord  DE  

Personen

Alle Personen

44

✓

42

 40



✗

2

 4

Nachname

Vorname

Firma

Organisationseinheit

Standort

Typ

Status

Alle

Alle



Historie: 

Report: 

Anzahl: 20 von 44

<< < Seite 1 von 3 > >>

Nachname	Vorname	Firma	Org			
Baschtus	Viavius	daccord	Engi			
Both	Ulvi	daccord	Exec			
Brehm	Britta	daccord	Cont			
Chang	Yen	daccord	Train			
Clarendice	Elizabeth	daccord	Acco			
Dold	Richard	daccord	Cont			
Forster	Jannett	daccord	Plan			
Ganzer	Peter	daccord	Train			
Hahn	Reiner	daccord	Cons			
Hanselmann	Heino	daccord	Purd			
Herzog	Aline	daccord	Accounting	Offenbach		✓
Juanez	Carlos	daccord	Marketing	Offenbach		✓
Kern	Julia	daccord	Sales	Offenbach		✓

admin, daccord  DE  

44

✓

42

 40



✗

2

 4

Typ

Status



Personen - Ansichten

Home Personen Active Directory Fileserver

Personen

Alle Personen

Nachname	Vorname	Firma	Organisationseinheit	Standort
Historie:				
Anzahl: 20 von 44				
Nachname	Vorname	Firma	Organisationseinheit	Standort
Baschtus	Viavius	daccord	Engineering	
Both	Ulvi	daccord	Executive Office	
Brehm	Britta	daccord	Contracting	Offenbach
Chang	Yen	daccord	Trainee	Offenbach
Clarendice	Elizabeth	daccord	Accounting	Offenbach
Dold	Richard	daccord	Contracting	Offenbach
Forster	Jannett	daccord	Planning	Offenbach
Ganzer	Peter	daccord	Trainee	Offenbach

 **Britta Brehm**

Identität

Personal-Nr.	100005
Vorname	Britta
Nachname	Brehm
Status	✓ Aktiv
Typ	 Interner Mitarbeiter
Benutzername	BBrehm

Organisation

Organisationseinheit	Contracting
Firma	daccord
Standort	Offenbach
Verantwortliche/r	Maximilian Meier

Kontakt

Telefon	
Mobile	
E-Mail	BBrehm@daccord.de



Personen - Ansichten

Home Personen Active Directory Fileserver

Administrator, Portal   

Personen

Alle Personen

 44 |  42 |  2 |  40 |  4 | 

Nachname	Vorname	Firma	Organisationseinheit	Standort	Typ	Status
					Alle 	Alle 

  Historie: 

Anzahl: von 44 « < Seite: von 3 > » Report: 

Nachname	Vorname	Firma	Organisationseinheit	Standort	Typ	Status
Baschtus	Viavius	daccord	Engineering	Offenbach		
Both	Ulvi	daccord	Executive Office	Offenbach		
Brehm	Britta	daccord	Contracting	Offenbach		
Chang	Yen	daccord	Trainee	Offenbach		
Clarendice	Elizabeth	daccord	Accounting	Offenbach		
Dold	Richard	daccord	Contracting	Offenbach		
Forster	Jannett	daccord	Planning	Offenbach		
Ganzer	Peter	daccord	Trainee	Offenbach		

Richtlinien zu Personen

Personen

Alle Personen

 44 |  42 |  40 |  3



2 kritische Richtlinien anzeigen

9 alle Richtlinien anzeigen

Inaktive Verantwortliche - Es gibt 1 inaktiven Verantwortlichen mit Verantwortung für aktive Personen.

Ausgeschiedene Personen mit Benutzerkonten - Es gibt 2 Personen (inaktiv und Austrittsdatum älter als 90 Tage) mit zugeordneten Konten.

Ungültiger Personenstatus - Es gibt 0 Personen mit einem ungültigem Wert im Feld: status.

Ungültiges Austrittsdatum - Es gibt 0 Personen mit einem ungültigen Wert im Feld: leavedate.

Personen in Selbstverantwortung - Es gibt 0 Personen die für sich selbst verantwortlich sind.

Aktive Personen ohne Verantwortlichen - Es gibt 0 aktive Personen ohne einen Verantwortlichen.

Ungültiger Personentyp - Es gibt 0 Personen mit einem ungültigen Wert im Feld: type.

Personen mit identischem Benutzernamen - Es gibt 0 Personen mit dem selben Benutzernamen.

Ausgeschiedene Personen mit Status aktiv - Es gibt 0 Personen (Austrittsdatum in der Vergangenheit) aber noch aktiv.

Richtlinien zu Personen – Status: kritisch

Inaktive Verantwortliche

Beschreibung:

Verantwortliche, die nicht mehr aktiv sind aber noch Mitarbeiter in der Verantwortung haben.

Auswertungsdetails:

Der importierte Datenbestand im Bereich Personen beinhaltet aktive Personeneinträge, bei denen die Information des Verantwortlichen (Feld: responsible) auf eine inaktive Person (Feld: status) verweist.

Empfehlung:

Angelehnt an gesetzliche Anforderungen und Empfehlungen im Bereich IT-Sicherheit / Identity Management sollte jede natürliche Person der Verantwortung durch eine andere natürliche Person unterliegen. Die verantwortliche Person kann dann Fragen zum Status einer Person beantworten oder, falls vorgeschrieben, die zyklische Bestätigung (Validierung oder Rezertifizierung) der Person durchführen. Weisen Sie den natürlichen Personen eine verantwortliche Person zu, die den Status "aktiv" besitzt, um Personen bewerten zu können und eine(n) Ansprechpartner(in) zu haben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt im IT Grundschutz Kompendium Artikel ORR4.M1 (Regelung für die Einrichtung von Benutzern und Benutzergruppen), dass Mitarbeiter einer verantwortlichen Person zugewiesen sein sollten, falls es zu einer erforderlichen Zustimmung oder Klärung zu bestimmten Thematiken kommt.

Es gibt 1 inaktiven Verantwortlichen mit Verantwortung für aktive Personen.



Nachname	Vorname	Berufsbezeichnung	Firma	Organisationseinheit	aktive Personen	Typ	Status
Rocker	Camilla	Department Lead Engineering	daccord	Engineering	1		

Ausgeschiedene Personen mit Benutzerkonten

Beschreibung:

Vervaltete Benutzerkonten sind mit hohen Risiken verbunden. Cyberhacker suchen oftmals nach diesen Konten, um sich einen Zugang auf Daten oder zu Systemen zu verschaffen.

Auswertungsdetails:

Es wurden Benutzerkonten gefunden, die ausgeschiedenen Personen zugewiesen sind. (inaktiv und seit mehr als 90 Tagen nicht mehr im Unternehmen)

Empfehlung:

Deaktivieren oder Löschen Sie sämtliche Zugriffsberechtigungen oder Konten des ausgeschiedenen Mitarbeiters (On Premises und cloudbasierte Systeme).

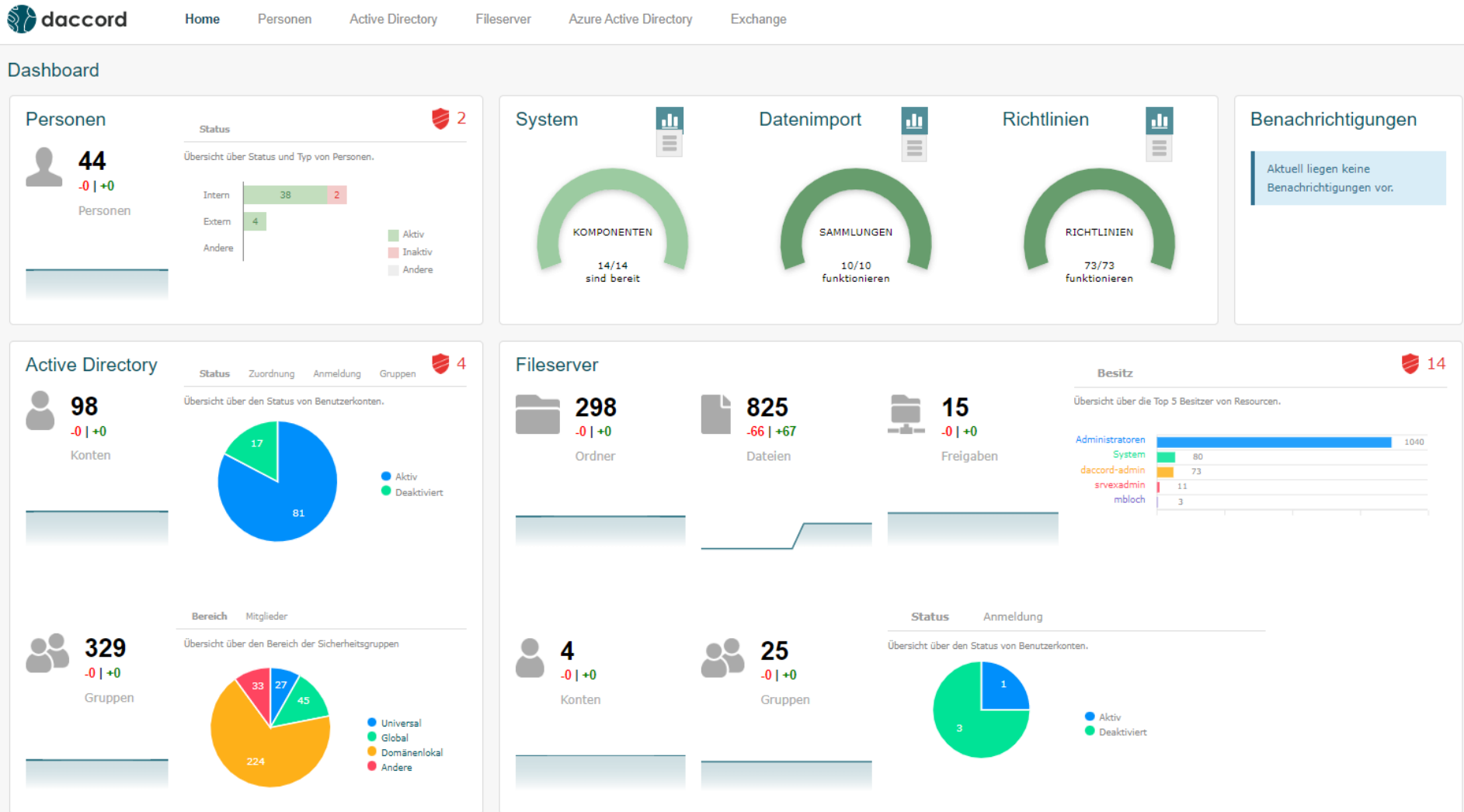
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt im IT Grundschutz Kompendium Artikel ORR4.M2 (Regelung für Einrichtung, Änderung und Entzug von Berechtigungen) nicht mehr benötigte Benutzerkonten zu sperren und dann zu löschen. Weitere Information finden Sie im Maßnahmenkatalog des BSI unter M 2.586 (Einrichtung, Änderung und Entzug von Berechtigungen).

Es gibt 2 Personen (inaktiv und Austrittsdatum älter als 90 Tage) mit zugeordneten Konten.



Nachname	Vorname	Berufsbezeichnung	Firma	Organisationseinheit	Konten	Austrittsdatum	Typ	Status
Rieke	Bettina	Construction Specialist	daccord	Contracting	1	31.01.2020		
Rocker	Camilla	Department Lead Engineering	daccord	Engineering	1	31.05.2020		

daccord – Microsoft Edition - DASHBOARD



Active Directory - Ansichten

 Home Personen **Active Directory** Fileserver Azure Active Directory Exchange admin, daccord DE

Active Directory

Alle User & Gruppen

  **98** User im Active Directory  **329** Gruppen im Active Directory

Active Directory	Username	Nachname	Vorname	Personenzuordnung	Letzte Nutzung	Status
DACCORD				Alle	Alle	Alle

Historie

Anzahl: 20 von 98

Report

Username	Nachname	Vorname	Domain	Letzte Nutzung	Status
\$H31000-GBQS82HKP6H			DACCORD	01.01.1601	
AAD_2df1c07cd025			DACCORD	17.08.2022	
AD\$			DACCORD	01.01.1601	
Administrator			DACCORD	13.01.2021	
AHerzog	Herzog	Aline	DACCORD	01.01.1601	
ASchmidt	Schmidt	Annegret	DACCORD	01.01.1601	
AVariz	Variz	Ahmed	DACCORD	07.10.2022	
BBrehm	Brehm	BrittaTest	DACCORD	01.01.1601	
BRieke	Rieke	Bettina	DACCORD	01.01.1601	
BVogel	Vodel	Belinda	DACCORD	01.01.1601	



Home

Personen

Active Directory

Fileservers

Azure Active Directory

Exchange

admin, daccordDE

Active Directory

Alle User & Gruppen

DACCORD

98User im
Active Directory

329Gruppen im
Active Directory

Active DirectoryUsernameNachnameVornamePersonenzuordnungLetzte NutzungStatus

DACCORD

Anzahl: 20 von 98

Username	Nachname	Vorname	Domain
\$H31000-GBQS82HKKP6H			DACCORD
AAD_2df1c07cd025			DACCORD
AD\$			DACCORD
Administrator			DACCORD
AHerzog	Herzog	Aline	DACCORD
ASchmidt	Schmidt	Annegret	DACCORD
AYariz	Yariz	Ahmed	DACCORD
BBrehm	Brehm	BrittaTest	DACCORD
BRieke	Rieke	Bettina	DACCORD
BVogel	Vodel	Belinda	DACCORD
		Carlos	DACCORD
		Carina	DACCORD
		Claudia	DACCORD
		Camilla	DACCORD
		daccord	DACCORD
		daccord-admin	DACCORD
			DACCORD
			DACCORD
		Elizabeth	DACCORD

BBrehm

Aktiver Person zugewiesen

DN

CN=Britta Brehm,OU=User_Standard_Intern,OU=Headquarter,OU=Organisation-DC=daccord.DC=de

sAMAccountName

BBrehm

Vorname

BrittaTest

Name

Brehm

Status

Aktiv

mehr Informationen

Erstellt am

26.01.2021

Geändert am

09.10.2022

Letzte Nutzung

01.01.1601

ObjectSid

S-1-5-21-1104076897-471672909-1837833638-1199

Domain

DACCORD

CN

Britta Brehm

userAccountControl

Value: 66048

- Standardaccount
- Das Kennwort läuft nicht ab

verknüpfte Ressourcen

Gruppen

Active Directory - Ansichten

Home Personen **Active Directory** FileserverAdministrator, Portal  DE  

Active Directory

 1 | 



 **94** User im Active Directory

 **329** Gruppen im Active Directory

UsernameNachnameVornamePersonenzuordnungLetzte NutzungStatus

Alle

Alle

Alle



 Historie: 

Report: 

Anzahl:

20

 von 94

<< < Seite: 1 von 5 >>

Username	Nachname	Vorname	Domain	Letzte Nutzung	Status
 \$H31000-GBQS82HKKP6H			DACCORD	01.01.1601	
 AAD_2df1c07cd025			DACCORD	26.12.2021	
 AD\$			DACCORD	01.01.1601	
 Administrator			DACCORD	13.01.2021	
 AHerzog	Herzog	Aline	DACCORD	01.01.1601	
 ASchmidt	Schmidt	Annegret	DACCORD	01.01.1601	



Richtlinien zu Active Directory

Active Directory

Alle User & Gruppen



4 kritische Richtlinien anzeigen

11 alle Richtlinien anzeigen

Domänenlokale Gruppen mit Benutzerkonten - Es gibt 33 Domänen-lokale Gruppen mit Benutzerkonten als Mitglieder.

Mit sich selbst verschachtelte Gruppen - Es gibt 2 Gruppen die mit sich selbst verschachtelt sind.

Große Anzahl an Domänen-Admins - Es gibt 6 Benutzerkonten mit Mitgliedschaft in der Gruppe: Domänen-Admins.

DFS-Gruppen mit Gruppenzuweisung außerhalb OU=Files Bereichs - Es gibt 19 DFS-Gruppen mit Gruppenzuweisung außerhalb OU=Files Bereichs

DFS-Gruppen ohne entsprechende MOD-READ F-Gruppen. - Es gibt 1 DFS-Gruppe ohne entsprechende MOD-READ F-Gruppen.

DFS-Gruppen mit zusätzlichen Gruppen außer .mod und .read - Es gibt 1 Gruppe mit zusätzlichen Gruppen außer .mod und .read

DFS-Gruppen mit Benutzern als Mitglied - Es gibt 1 DFS-Gruppe mit Benutzern als Mitglied

Mod-Read-Gruppen mit Gruppenzuweisungen - Es gibt 1 Mod/Read Gruppe mit zusätzlichen Gruppenzuweisungen

DFS-Gruppen ohne Rechte auf den zugehörigen Ordner - Es gibt 4 DFS-Gruppen ohne Berechtigungen auf den entsprechenden Ordner

DFS-Gruppen außerhalb des OU=File Bereichs - Es gibt 4 DFS-Gruppen außerhalb des OU=Files Bereichs

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

Richtlinien zu Active Directory

Active Directory

Alle User & Gruppen

1

4 kritische Richtlinien anzeigen

11 alle Richtlinien anzeigen

Domänenlokale Gruppen mit Benutzerkonten - Es gibt 33 Domänen-lokale Gruppen mit Benutzerkonten als Mitglieder.

Mit sich selbst verschachtelte Gruppen

Große Anzahl an Domänen-Admins

DFS-Gruppen mit Gruppenzuweisung außerhalb OU=Files Bereichs

DFS-Gruppen ohne Gruppenzuweisung

DFS-Gruppen mit Gruppenzuweisung innerhalb OU=Files Bereichs

DFS-Gruppen mit Gruppenzuweisung außerhalb OU=Files Bereichs

Mod-Read-Gruppen

DFS-Gruppen ohne Gruppenzuweisung

DFS-Gruppen außerhalb OU=Files Bereichs

Zu viele Gruppenmitglieder

Active Directory

Alle User & Gruppen

4 kritische Richtlinien anzeigen

11 alle Richtlinien anzeigen

Domänenlokale Gruppen mit Benutzerkonten - Es gibt 33 Domänen-lokale Gruppen mit Benutzerkonten als Mitglieder.

Mit sich selbst verschachtelte Gruppen - Es gibt 2 Gruppen die mit sich selbst verschachtelt sind.

Große Anzahl an Domänen-Admins - Es gibt 6 Benutzerkonten mit Mitgliedschaft in der Gruppe: Domänen-Admins.

DFS-Gruppen mit Gruppenzuweisung außerhalb OU=Files Bereichs - Es gibt 19 DFS-Gruppen mit Gruppenzuweisung außerhalb OU=Files Bereichs

d

Richtlinien zu AD mit dem Status – kritisch

 daccord

Home

Personen

Active Directory

Fileserver

Administrator, Portal

DE





Active Directory

Alle User & Gruppen



4 kritische Richtlinien anzeigen

Domänenlokale Gruppen mit Benutzer...

Mit sich selbst verschachtelte Gruppen...

Große Anzahl an Domänen-Admins...

DFS-Gruppen mit Gruppenzuweisung...

 **Mit sich selbst verschachtelte Gruppen**

Beschreibung:

Active Directory Gruppen, welche mit sich selbst verschachtelt sind, können innerhalb von Anwendungen oder Scripten zu Problemen führen.

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 2 Gruppen die mit sich selbst verschachtelt sind.





Gruppenname	ID
G_IT_Departmentlead	CN=G_IT_Departmentlead,OU=Global Groups,OU=Headquarters
G_Marketing_Departmentlead	CN=G_Marketing_Departmentlead,OU=Global Groups,OU=Headquarters

NTFS - Ansichten

 [Home](#) [Personen](#) [Active Directory](#) **Fileserver**

Administrator, Portal  DE  

Fileserver  3 

Alle Fileserver

 3 verschiedene Fileserver

 986 Ordner auf dem Fileserver

 0 lokale User auf dem Fileserver

 0 lokale Gruppen auf dem Fileserver

Fileserver User und Gruppen Shares, Ordner und Dateien

Alle 



Name

 GUHTESTSRV002

 GUHTESTSRV001

 GUHTESTMEM001

NTFS - Ansichten

 **daccord**

Home Personen Active Directory **Fileserver**

Administrator, Portal  

Fileserver

Alle Fileserver



13 kritische Richtlinien anzeigen

20 alle Richtlinien anzeigen

Benutzerkonten mit Vollzugriff - Es gibt 6 Benutzerkonten mit Vollzugriffs-Berechtigungen.

Nicht auswertbare Datenbereiche - Es gibt 379 Verzeichnisse oder Dateien, bei denen die Sicherheitsinformationen nicht ausgelesen werden konnten.

Pfadlänge zu lang - Es gibt 30 Verzeichnisse, bei denen die maximale Pfadlänge überschritten oder erreicht ist.

Andere Besitzer als "Administratoren" oder "System" - Es gibt 4239 Ordner oder Dateien mit anderen Besitzern als die Gruppe "Administrators" oder "System".

Benutzerkonten mit direkten Berechtigungen - Es gibt 10 Benutzerkonten mit direkten Berechtigungszuweisungen zu Ordnern oder Dateien.

Datenbereiche mit unterbrochener Vererbung - Es gibt 23 Ordner bei denen die Vererbung unterbrochen ist.

Ordner der 2. Ebene mit direkt vergebenen Userberechtigungen - Es gibt 14 Ordner der 2. Ebene mit direktem Userzugriff

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

Berechtigungen für "Jeder" - Es gibt 9 Ordnern, Dateien oder Freigaben auf welche die Gruppe "Jeder" Berechtigungen besitzt.

Globale Gruppen mit direkten Berechtigungen - Es gibt 1 globale Gruppe mit Berechtigungen.

Freigaben ohne Ursprungsordner - Es gibt 7 Freigaben, bei denen der relevante Ordner nicht existiert.

Ordner der 2. Ebene ohne System- oder Administratorenzugriff - Es gibt 12 Ordner der 2. Ebene ohne System- oder Administratorenzugriff

NTFS - Ansichten

 **daccord**

HomePersonenActive DirectoryFileserver

Administrator, PortalDE

Benutzerkonten mit Vollzugriff

Beschreibung:
Benutzerkonten mit Vollzugriff auf Datenbereiche können innerhalb dieses Bereiches auch die Zugriffsrechte und den Besitzer verändern. Diese speziellen Berechtigungen werden für den lesenden und schreibenden Zugriff auf Ordner und Dateien nicht benötigt und sollten nur in Ausnahmefällen vergeben werden.

Auswertungsdetails:
In Ihrer Umgebung wurden Benutzerkonten mit der Berechtigung „Vollzugriff“ auf Ordner oder Dateien gefunden.

Empfehlung:
Generell sollte man mit der NTFS Berechtigung "Vollzugriff" vorsichtig umgehen. Es empfiehlt sich, mit den NTFS Berechtigungen "Ändern", "Lesen" und "Schreiben" zu arbeiten. Mit diesen Berechtigungen können keine Berechtigungen oder die Besitzerfunktion geändert werden. Über die Berechtigung "Vollzugriff" sollten nur Administratoren verfügen.

Es gibt 6 Benutzerkonten mit Vollzugriffs-Berechtigungen.



System	Benutzername	ID	Nachname	Vorname	Zuletzt benutzt	Anzahl Ordner	Anzahl Dateien	Status
DACCORD	Administrator	CN=Administrator,CN=Users,DC=daccord,DC=de			13.01.2021	1	0	✓
DACCORD	mrudolph	CN=Max Rudolph,OU=IT,OU=G&H,OU=Organisation,DC=daccord,DC=de	Rudolph	Max	03.03.2022	1	0	✓
DACCORD	MSchmidt	CN=Martin Schmidt,OU=User_Sicherheit,OU=Headquarter,OU=Organisation,DC=daccord,DC=de	Schmidt	Martin	01.01.1601	1	0	✓
DACCORD	GSchmidtmeier	CN=Gisela Schmidtmeier,OU=User_Standard_intern,OU=Headquarter,OU=Organisation,DC=daccord,DC=de	Schmidtmeier	Gisela	01.01.1601	1	0	✓
DACCORD	daccord-admin	CN=daccord-admin,OU=IT,OU=G&H,OU=Organisation,DC=daccord,DC=de		daccord-admin	07.03.2022	26	6	✓
DACCORD	PKinzinger	CN=Petra Kinzinger,OU=Users,OU=DAC - Daccord Action Company,OU=Organisation,DC=daccord,DC=de	Kinzinger	Petra		1	0	✓

MS Exchange - Ansichten

 Home Personen Active Directory Fileserver Azure Active Directory **Exchange**

admin, daccord DE

Exchange

Alle Mailboxen & Verteilerlisten

 **Exchange**

 **25** Mailboxen in Exchange

 **8** Verteilerlisten in Exchange

Exchange System

Name

Kategorie

Personenzuordnung

Exchange

Alle

Alle

Report

Anzahl: 20 von 25

Name	Exchange System	Kategorie	Alternative Email Adressen	Mailboxgröße	Letzte Anmeldung
✓ AHerzog@daccord.de	Exchange	Benutzer Mailbox	1	479.70 KB	
✓ AYariz@daccord.de	Exchange	Benutzer Mailbox	1	479.62 KB	23.11.2021
✓ BBrehm@daccord.de	Exchange	Benutzer Mailbox	1	0 Byte	
✗ BVogel@daccord.de	Exchange	Benutzer Mailbox	1	0 Byte	
✓ CJuarez@daccord.de	Exchange	Benutzer Mailbox	1	737.80 KB	05.11.2021
✓ CPiller@daccord.de	Exchange	Benutzer Mailbox	1	0 Byte	
✓ CRocker@daccord.de	Exchange	Benutzer Mailbox	1	77.42 KB	
✗ DiscoverySearchMailbox:{D919BA05-46A6-415F-80AD-7E09334BB852}@daccord.de	Exchange	Discovery Mailbox	1	65.29 KB	

MS Exchange - Details

Home Personen Active Directory Fileserver Azure Active Directory **Exchange**

Exchange

Alle Mailboxen & Verteilerlisten

 **Exchange**

 **25** Mailboxen in Exchange

 **8** Verteilerlisten in Exchange

Exchange System

Name

Kategorie

Personenzuordnung

Exchange

Alle

Alle

Historie:

Anzahl: 20 von 25

Name	Exchange System	Kategorie	Alternative E-Mail-Adressen
 srhexadmin@daccord.de	Exchange	Benutzer Mailbox	1
 skornblueh@daccord.de	Exchange	Benutzer Mailbox	1
 AYariz@daccord.de	Exchange	Benutzer Mailbox	1
 CRocker@daccord.de	Exchange	Benutzer Mailbox	1
 PWollmann@daccord.de	Exchange	Benutzer Mailbox	1
 Neumann@daccord.de	Exchange	Benutzer Mailbox	1
 mbloch@daccord.de	Exchange	Benutzer Mailbox	1

 **AYariz@daccord.de**

  ✓ Aktiver Person zugewiesen

ObjectSid

a5291987-1869-4f6f-88a0-7d8b31d4f5b7

Mailbox ID

AYariz@daccord.de

sAMAccountName

AYariz

Name

AYariz@daccord.de

Anzeigenname

Ahmed Yariz

Besitzer

AYariz

Exchange System

Exchange

Kategorie

Benutzer Mailbox

Datenbank

DB1

E-Mail Adressen

▲

Weitere Attribute

▲

Berechtigungen

▲

Verteilerlisten

▲



MS Exchange - Details

Home Personen Active Directory Fileserver Azure Active Directory Exchange

Exchange

Alle Mailboxen & Verteilerlisten

 **Exchange**

 **25** Mailboxen in Exchange

 **8** Verteilerlisten in Exchange

Exchange System	Name	Kategorie	Personenzuordnung
Exchange			

Historie: 

Anzahl: 20 von 25

Name	Exchange System
 srhexadmin@daccord.de	Exchange
 skornblueh@daccord.de	Exchange
 AYariz@daccord.de	Exchange
 CRocker@daccord.de	Exchange
 PWollmann@daccord.de	Exchange
 Neumann@daccord.de	Exchange
 mbloch@daccord.de	Exchange

Weitere Attribute

Maximale Empfangsgröße	Nicht limitiert
Maximale Sendegröße	Nicht limitiert
Sperre für Senden	819.20 MB
Sperre für Empfangen	1.00 GB
Belegter Speicher	479.62 KB
Verborgen von Adressliste	Nein
Letzte Nutzung	23.11.2021
Erstellt am	26.01.2021
Geändert am	07.10.2022

 **AYariz@daccord.de**

  ✓ Aktiver Person zugewiesen

ObjectSid	a5291987-1869-4f6f-88a0-7d8b31d4f5b7
Mailbox ID	AYariz@daccord.de
sAMAccountName	AYariz
Name	AYariz@daccord.de
Anzeigenname	Ahmed Yariz
Besitzer	AYariz
Exchange System	Exchange
Kategorie	Benutzer Mailbox
Datenbank	DB1

E-Mail Adressen

Weitere Attribute

Berechtigungen

Verteilerlisten



MS Exchange - Richtlinien

 [Home](#) [Personen](#) [Active Directory](#) [Fileserver](#) [Azure Active Directory](#) [Exchange](#)

admin, daccord   

Exchange

Alle Mailboxen & Verteilerlisten

 1 



2 kritische Richtlinien anzeigen

13 alle Richtlinien anzeigen

Unbenutzte Mailboxen - Es gibt 13 Mailboxen, die vor mehr als 6 Monaten erstellt wurden und noch unbenutzt sind

Letzte Anmeldung vor mehr als 6 Monaten - Es gibt 8 Mailboxen, die zuletzt vor mehr als 6 Monaten genutzt wurden

Weiterleitung nach extern - Es gibt 1 Mailbox, die eine Weiterleitung nach extern eingerichtet hat.

Maximale Speicherkapazität fast erreicht - Es gibt 0 Mailboxen, deren maximale Speicherkapazitäten fast erreicht sind

Zu viele Berechtigungen - Es gibt 0 Benutzerkonten, bei denen die maximale Anzahl (max. 10) an Berechtigungen überschritten oder erreicht sind.

Nur inaktive User - Es gibt 0 Mailboxen, die nur inaktive Benutzer haben

Zu viele Verteilergruppenmitgliedschaften - Es gibt 0 Benutzerkonten, bei denen die maximale Anzahl (max. 10) an Mitgliedschaften in Verteilergruppen überschritten oder erreicht sind.

Verteilergruppen ohne Manager - Es gibt 0 Verteilergruppen, die keine Manager haben.

Verschachtelte Berechtigungen auf Mailboxen - Es gibt 0 Benutzerkonten mit verschachtelten Berechtigungen

Verteilergruppen ohne Mitglieder - Es gibt 0 Verteilergruppen, die keine Mitglieder haben.

Verteilergruppen mit inaktiven Mitgliedern - Es gibt 0 Verteilergruppen mit inaktiven Mitgliedern

Mailboxen ohne Berechtigungen - Es gibt 0 Mailboxen, die keine Berechtigungen haben.

Verteilergruppen mit inaktivem Manager - Es gibt 0 Verteilergruppen mit inaktiven Managern

MS Exchange - Richtlinien

daccord Home Personen Active Directory Fileserver Azure Active Directory Exchange admin, daccord DE

Exchange

Alle Mailboxen & Verteilerlisten

2 kritische Richtlinien anzeigen

Alle Mailboxen & Verteilerlisten

2 kritische Richtlinien anzeigen

13 alle Richtlinien anzeigen

Unbenutzte Mailboxen - Es gibt 13 Mailboxen, die vor mehr als 6 Monaten erstellt wurden und noch unbenutzt sind

Letzte Anmeldung vor mehr als 6 Monaten - Es gibt 8 Mailboxen, die zuletzt vor mehr als 6 Monaten genutzt wurden

Weiterleitung nach extern - Es gibt 1 Mailbox, die eine Weiterleitung nach extern eingerichtet hat.

Maximale Speicherkapazität fast erreicht - Es gibt 0 Mailboxen, deren maximale Speicherkapazitäten fast erreicht sind

Zu viele Berechtigungen - Es gibt 0 Benutzerkonten, bei denen die maximale Anzahl (max. 10) an Berechtigungen überschritten oder erreicht sind.

Unbenutzte Mailboxen - Es gibt 13 Mailboxen, die vor mehr als 6 Monaten erstellt wurden und noch unbenutzt sind

Letzte Anmeldung vor mehr als 6 Monaten - Es gibt 8 Mailboxen, die zuletzt vor mehr als 6 Monaten genutzt wurden

Weiterleitung nach extern - Es gibt 1 Mailbox, die eine Weiterleitung nach extern eingerichtet hat.

Maximale Speicherkapazität fast erreicht - Es gibt 0 Mailboxen, deren maximale Speicherkapazitäten fast erreicht sind

Zu viele Berechtigungen - Es gibt 0 Benutzerkonten, bei denen die maximale Anzahl (max. 10) an Berechtigungen überschritten oder erreicht sind.

MS Exchange - Richtlinien

Unbenutzte Mailboxen

Beschreibung:

Mailboxen, an die sich noch nie angemeldet wurde, könnten auf verwaiste Konten hinweisen. Verwaiste Konten weisen ein hohes Sicherheitsrisiko auf und bieten Angreifern einen möglichen Zugriff auf das System.

Auswertungsdetails:

Das Exchange System beinhaltet Mailboxen, die noch nie benutzt wurden und deren Erstellung (Feld: created) mehr als 6 Monate zurückliegt.

Empfehlung:

Es wird empfohlen zu überprüfen, warum die Mailbox noch nie benutzt wurde. Sollte es sich um ein verwaistes Konto handeln, wird empfohlen, die Mailbox zu entfernen.

Es gibt 13 Mailboxen, die vor mehr als 6 Monaten erstellt wurden und noch unbenutzt sind



Name	Kategorie	Anzeigenname	Besitzer
AHerzog@daccord.de	UserMailbox	Aline Herzog	AHerzog
BBrehm@daccord.de	UserMailbox	Britta Brehm	BBrehm
BVogel@daccord.de	UserMailbox	Belinda Vodel	BVogel
CPiller@daccord.de	UserMailbox	Claudia Piller	CPiller
CRocker@daccord.de	UserMailbox	Camilla Rocker	CRocker



Access Governance
„Made in Germany“

Vielen Dank für Ihre Aufmerksamkeit!