

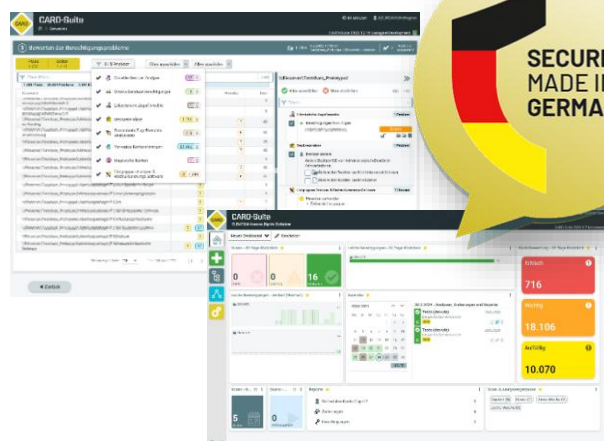


Version 2026.9

Handbuch

Benutzerhandbuch der CARO-Suite

Analysieren, Automatisieren,
Kontrollieren und Dokumentieren
mit der CARO-Suite





Inhaltsverzeichnis

Installation und Konfiguration	5
Systemvoraussetzungen.....	5
Einfache Installation und Inbetriebnahme.....	5
Update-Installation.....	5
CARO-Suite - WebClient.....	5
Start-Bildschirm.....	7
Vorschaufunktionen	8
Konfigurationsmanager	8
Zugangskonten konfigurieren.....	8
Neue Anmeldung erstellen.....	8
Einstiegspunkte konfigurieren	9
Filesystem-Einstiegspunkte.....	9
Microsoft Entra ID Anbindung	14
Active Directory Einstiegspunkte.....	14
AD-Security Events überwachen mit dem Observer.....	15
Observer-Konfiguration.....	16
Globale Einstellungen	18
Smart Permissions©.....	18
Benutzereinstellungen.....	19
Analysieren und Bereinigen.....	20
Funktionsübersicht	20
Die Bereinigungsbausteine und ihre Anwendungsfälle.....	21
Risikoeinstufung der Analysen.....	21
Analysen mit Risikoeinstufung kritisch	22
Analysen mit Risikoeinstufung wichtig.....	23
Analysen mit Risikoeinstufung auffällig.....	24
Anpassung der Risikoeinstufungen.....	26
Das CARO-Dashboard	26
Default-Dashboard.....	26
Dashboard bearbeiten	27
Widget-Größe ändern.....	27
Ein neues Widget hinzufügen.....	28
Ein neues Dashboard erzeugen.....	28
Die Widgets und ihre Funktion	29
Neue Bereinigung: In 5 Schritten Ihr System bereinigen.....	38



Schritt 1: Einen Scan konfigurieren	38
Schritt 2: Risikobewertung und Analyse	41
Schritt 3: Bewerten der Probleme	45
Schritt 4: Bereinigen	45
Schritt 5: Dokumentieren	46
Scan und Analysen wiederkehrend planen	47
Scans wiederkehrend planen	48
Auf einer bestehenden Analyse aufsetzen	49
Was sind „Elemente aus gelöschten Analysen“?	50
Weiter Aufräumen nach einer durchgeführten Analyse	50
Nach einigen Bereinigungen weiter aufräumen	50
Reporte anzeigen oder herunterladen	50
Dokumentieren	52
Funktionsüberblick	52
Globale Einstellungen für Reporte	53
Automatisieren	55
Funktionsübersicht	55
Automatisches Bereinigen mit der CARO-Suite	56
Fortschritts-Anzeige	56
Konfiguration	57
Bei Bewertungsvorschau anhalten (nur Bewerten)	57
Speicherbedarf minimieren	59
Ergebnisse	59
Ressourcen-Ansicht zur Berechtigungsanalyse	60
Live-Anzeige der Ist-Berechtigungen	61
Direktes Berechtigungsmanagement	61
Berechtigungsreporte erstellen	62
Von einem Konto in die Kontenansicht navigieren	62
Eine IST-Berechtigungsanalyse starten	62
Anzeige von Berechtigungs-Anomalien	64
Verteilung von Berechtigungen (Statistiken)	64
Anzeige der Berechtigungskategorien	66
Berechtigungs-Reporte	68
Erstellen von umfangreichen Reporten	71
Verwalten mit der CARO-Suite	72
Verfügbare Technologien	72



Verwaltung im Filesystem	72
Verwaltung im Active Directory.....	73
Verwalten im Entra ID	74
Verwalten im Exchange	74
Verwaltungsaufgaben-Übersicht	74
Aufbewahrung von Verwaltungsaufgaben	75
Berechtigungen ändern	76
Ansicht	76
Anpassung der sichtbaren Kategorien	76
Berechtigungsänderungen per Drag&Drop	77
Konten-Ansicht mit Suchfunktion	78
Anzeigemodus wählen.....	78
Suche konfigurieren.....	79
Excel-Kontenreport erzeugen.....	80
Mitgliedschaftsbeziehungen darstellen.....	80
Graphische Anzeige der direkten und indirekten Pfade	81
Globales Logbuch	84
Gründe für die Nutzung.....	84
Quellen.....	85
Details – Was wird angezeigt.....	85
Filtern nach Zeiträumen	85
Suche	86
Weitere Funktionen.....	87
Logbucheinträge an Objekten.....	87
CUSATUM Service GmbH.....	89
Herausgeber	89
Support	89

50	14	32	6	23
Analysen	Bausteine	Verwaltungsaufgaben	Technologien	Releases



Installation und Konfiguration

Systemvoraussetzungen

Die Caro-Suite setzt bestimmte Systemvoraussetzung voraus, um eine erfolgreiche und performante Installation und Benutzung zu gewährleisten. Detaillierte Informationen zu den Minimalanforderungen für den reibungslosen Betrieb finden sie in unserem Handbuch **CARO-Suite Systemvoraussetzungen.pdf**.

Einfache Installation und Inbetriebnahme

Die Installation und Inbetriebnahme der CARO-Suite ist in wenigen Schritten abgeschlossen, so dass Sie erste Ergebnisse in den Views in weniger als 10 Minuten sehen.

Im Handbuch **CARO-Suite-Configurator-Handbuch.pdf** ist eine Schritt-für-Schritt-Anleitung beschrieben, wie Sie schnell und einfach die CARO-Suite vor der ersten Benutzung konfigurieren.

Diese Themen werden ausführlich behandelt:

- Lizenzdatei einspielen
- MS-SQL-Datenbank-Einrichtung
- IIS-Konfiguration mit Zertifikatsbehandlung
- Web-Client-Einrichtung
- Benutzermanagement

Update-Installation

Nach dem Sie ein neues Versionspaket der CARO-Suite installiert haben, öffnet sich der WebClient und zeigt Ihnen aktuelle Hinweise zum Update-Prozess an. Hier werden Ihre vorhandenen Datenbanken überprüft und ggf. einem Update unterzogen. Bitte warten Sie den Prozess ab. In sehr großen Systemen kann dies einige Minuten in Anspruch nehmen.

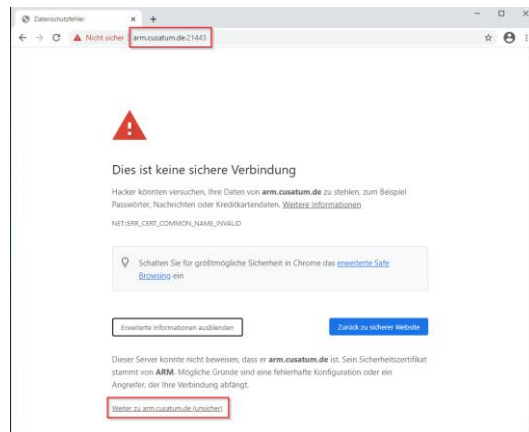


CARO-Suite erledigt noch ein paar die Dinge für Sie. Bitte bleiben Sie dran...

CARO-Suite – WebClient

Starten Sie den WebClient über den Chrome/Edge (mit Chrome) oder Firefox. IE 11 wird nicht unterstützt. Die Adresse ist **<https://caro-server.fqdn.de>** oder **<https://caro-server.fqdn.de:21443>**.

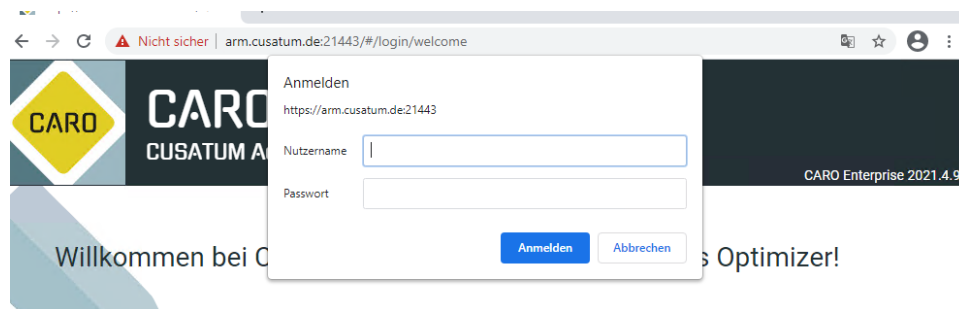
Wenn ein Self-Sign-Zertifikat benutzt wurde, dann muss das „Risiko“ akzeptiert werden.



Danach müssen für SSO einmalig die Credentials eingegeben werden oder die Seite muss als vertrauenswürdig eingetragen werden.

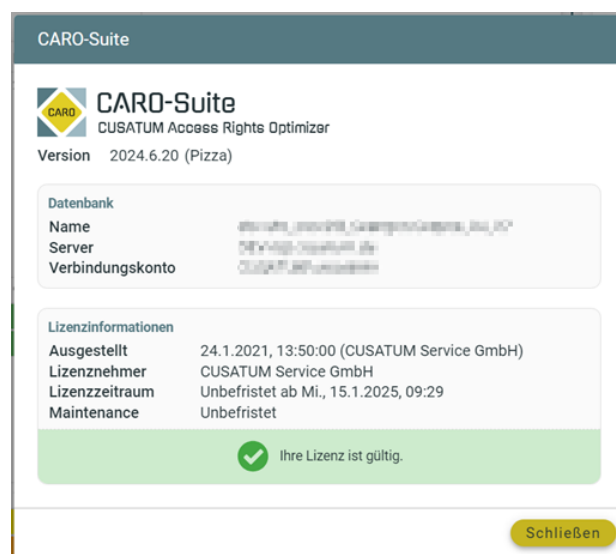


Achtung: Nach der ersten Installation muss der Benutzer, welcher sich in das Benutzer-Management eingetragen hat, sich nochmal ab- und wieder anmelden. Alternativ kann der CARO-Service auch rebootet werden.



Nach dem erfolgreichen Login steht Ihnen die CARO-Suite nun zur Verfügung.

Die Lizenz-Informationen für Ihre CARO-Suite können Sie jederzeit über das User-Menü (nach dem Login verfügbar) oder im Login-Fenster selbst oben rechts über das Menü  öffnen:



Versions- und Lizenzdialog der CARO-Suite



Start-Bildschirm

Auf dem Start-Bildschirm der CARO-Suite sehen Sie nach einer erfolgreichen Installation und Erstkonfiguration Hinweise auf die nächsten Schritte.

Willkommen bei CARO - dem CUSATUM Access Rights Optimizer!

Erste Schritte

① Scan konfigurieren

- Einstiegspunkte und ihre Scan-Parameter einrichten
- Anmeldedaten zum Scannen und Ändern eingeben
- Aufgabe für eine Bereinigung auswählen

② Analysieren und Bewerten der Berechtigungsprobleme

- CARO zeigt nach dem Scan alle Berechtigungsprobleme auf, wo sich unaufgelöste Berechtigungseinträge oder verwaiste Besitzer befinden

③ Bereinigen der Berechtigungsprobleme

- Führe erste Bereinigungen durch
- z.B. unterbrochene Vererbung bei verschobenen Verzeichnissen korrigieren oder verwaiste SIDs entfernen
- oder Direktberechtigungen mit automatisierten Bulk-Operationen korrigieren

1

Konfigurieren Sie Ihr System für eine erste Analyse.

✓

Anmeldedaten

!

Es wurden noch keine Einstiegspunkte konfiguriert.

2

Analysieren und Bewerten der Berechtigungsprobleme

DB

Starten Sie Ihren ersten Scan

LIVE

Starten Sie Ihre erste Live-Abfrage

Der **1. Schritt** ist das Einrichten Ihrer Scan-Einstiegspunkte im Konfigurationsmanager. Es empfiehlt sich das Einrichten eines Domänen-Scans (Active Directory-Einstiegspunkt), sowie eine bis mehrere Filesystem-Einstiegspunkte. Nachdem Sie Ihre gewünschten Scan-Einstiegspunkte erzeugt haben, können Sie im **2. Schritt** einen ersten Scan konfigurieren und den Scan mit einer ersten Risiko-Bewertung starten. Eine Anleitung dazu finden Sie im Kapitel [Schritt 1: Einen Scan konfigurieren](#).

Alternativ zu einem ersten Scan können Sie die Live-Kontenansicht und die Live-Ressourcen-Ansicht nutzen, um in Echtzeit Konten und Berechtigungen einzusehen.

1

Konfigurieren Sie Ihr System für eine erste Analyse.

✓

Anmeldedaten

✓

Einstiegspunkte

AD

✓

AD Einstiegspunkt konfiguriert

FS

✓

FS Einstiegspunkt konfiguriert

Andere

!

Andere Einstiegspunkte noch nicht konfiguriert

2

Analysieren und Bewerten der Berechtigungsprobleme

DB

Starten Sie Ihren ersten Scan

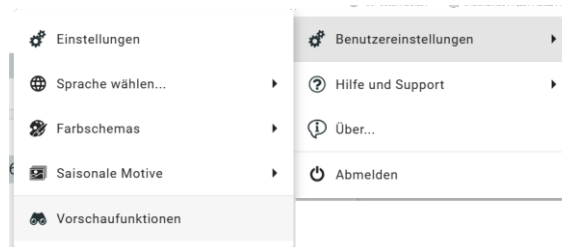
LIVE

Starten Sie Ihre erste Live-Abfrage



Vorschaufunktionen

Mit der CARO-Vorschaufunktion erhalten unsere Kunden einen ersten exklusiven Eindruck von neuen Funktionen in der CARO-Suite. Schauen Sie also ab- und zu nach einem Update Ihrer CARO-Suite in die Liste der Vorschaufunktionen.

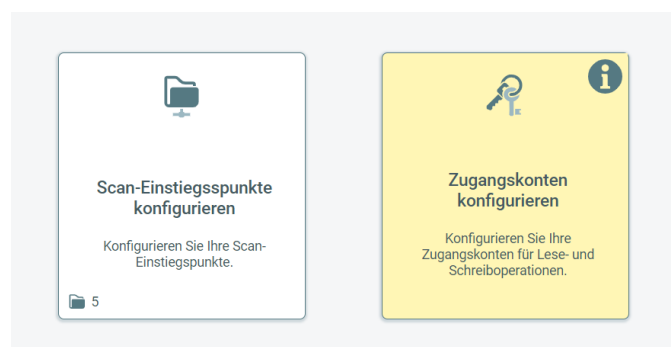


Konfigurationsmanager

Zugangskonten konfigurieren

In Abhängigkeit der verwendeten Technologien benötigen alle Arbeitsprozesse, Lese- und Schreiboperationen sowie generelle Änderungen, ein oder mehrere Konten. Aus diesem Grund ist die Konfiguration der Zugangskonten der erste Schritt.

Wir empfehlen an dieser Stelle die Verwendung von dedizierten Service-Accounts. Liegen diese bei der ersten Installation noch nicht vor, so können diese später nachgetragen werden.



*Ansicht des Konfigurationsmanagers,
es wurden noch keine Zugangskonten konfiguriert*

Neue Anmeldung erstellen

Ist die Zugangskonfiguration geöffnet, muss mindestens ein Account hinterlegt werden, der berechtigt ist, alle gewünschten Änderungen auf den Systemen durchzuführen.

Die Accounteingabe wird über den Dialog **Anmeldedaten eingeben** realisiert, der alle relevanten Daten erfasst und abspeichert.

Anmeldedaten erstellen

Benutzername

TheTestUser

Domäne

cusatum

Kennwort

••••••••

Speichern

Abbrechen

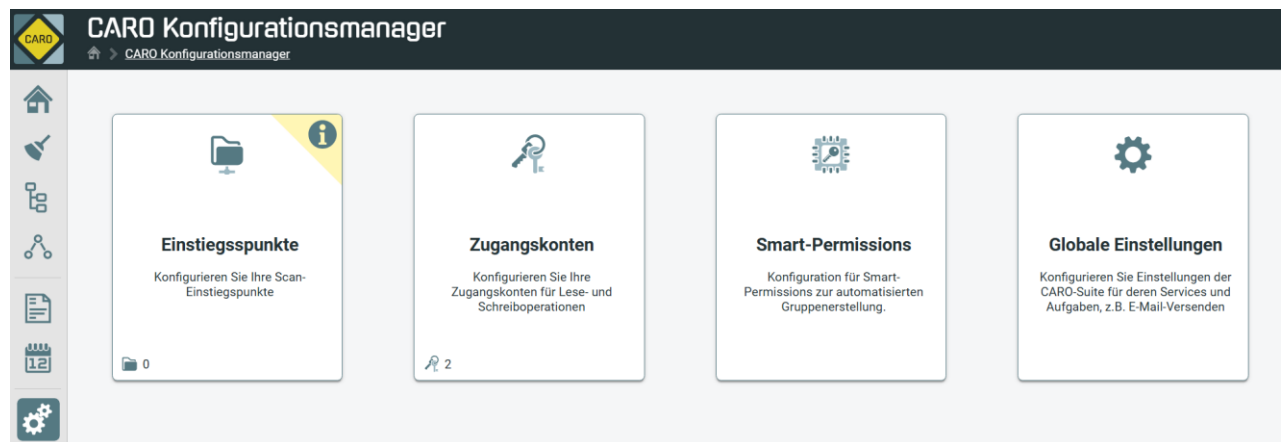


Anschließend haben Sie für den zukünftigen Gebrauch alle hinterlegten Zugangskonten in einer tabellarischen Übersicht erfasst:

Filtern...		2
Benutzername	Domäne	
system	workgroup	
MeinAdminKonto	system0815	

Einstiegspunkte konfigurieren

Die Einstiegspunkte der CARO-Suite stellen die Startpunkte für Ihre Scans und Analysen dar. Sie können hier mehrere Einstiegspunkte konfigurieren, z.B. Shares, ganze Fileserver oder einzelne Verzeichnisse.



Konfigurationsmanager mit den einzelnen Gruppen

Handelt es sich um eine Erstinstallation, werden Sie noch keine Einstiegspunkte besitzen. Hier legen wir zuerst einen neuen Einstiegspunkt an.

Filesystem-Einstiegspunkte

Hier können Sie Ihre Fileserver, Freigaben oder einzelne Verzeichnisse für Ihre Analysen oder Bereinigungen konfigurieren. **DFS-Shares** können ebenfalls konfiguriert werden.



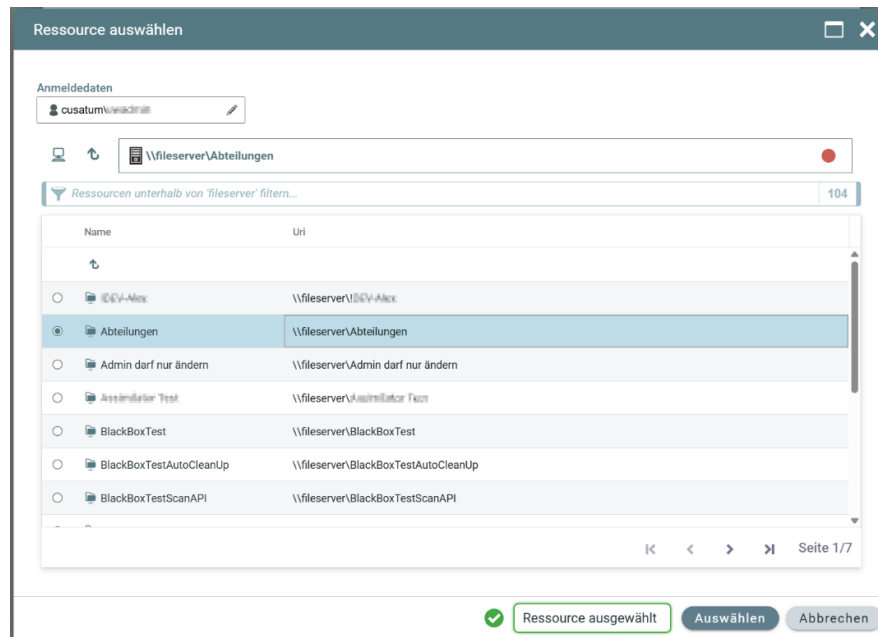
Einstiegspunkte-Konfiguration für einen Share

Alle notwendigen Systeminformationen werden hier hinterlegt. Dazu gehören:

- Der UNC-Pfad – Pfad zum Share oder Fileserver, der gescannt und bereinigt werden soll.
- Der Name – wird intern für diese Konfiguration verwendet, er ist frei wählbar und kann angepasst werden.
- Anmeldedaten – Mit diesem hinterlegten Service-Konto werden der Scan, die Analyse und die Änderungen durchgeführt.
- Die Scantiefeneinstellung – Zur Begrenzung der Scantiefe und Optimierung des DB-Speicherverbrauchs.
- Lokale Konten mitscannen – auch die lokalen Konten werden mitgescannt, diese werden dann u.a. in der Ressourcen-Ansicht mit ihren Informationen angezeigt.
- Ausschlussliste – Definieren Sie hier ein regex-Pattern zum Ausschluss (Blacklist) von nicht zu scannenden Bereichen, z.B.: `^\\\\\\\\\\\\\\\\\\\\Servername\\\\\\\\\\\\(Users$|Users\\\\\\\\\\\\.*)`
Diese Einstellung ist derzeit als Vorschau-Feature integriert und muss erst freigeschaltet werden (siehe Kapitel [Vorschau-Features](#)).
- Performance-Plan – Einstellung der Scanleistung, Standard ist Höchstleistung, d.h. es werden 32 Abfragen gleichzeitig auf den Zielressourcen durchgeführt, Die Belastung der CPU-Cores auf dem Zielsystem kann durch diese Einstellung beeinflusst werden.

System live durchsuchen

Über die Schaltfläche „Durchsuchen“ können Sie Ihren aktuellen Fileserver, Freigabe, Verzeichnis oder eine Domäne suchen und als neuen Scan-Einstiegspunkt auswählen:



Auswahl einer Ressource als Einstiegspunkt zum Scannen und Analysieren

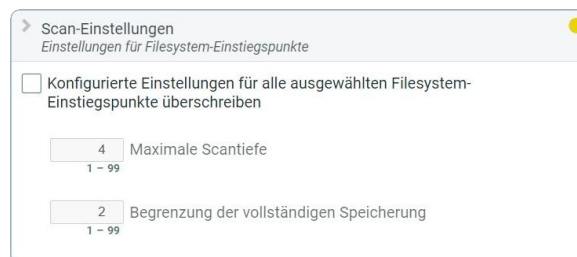
Scantiefeneinstellungen

Sie können festlegen, wie tief Sie Ihre Ordnerstrukturen scannen und analysieren wollen mit der maximalen Scantiefe. Der Standardwert ist 10. Zusätzlich können Sie bestimmen, bis zu welcher Ebene CARO vollständig seine Daten speichern soll: Die Ebenen für eine vollständige Speicherung aller gesammelten Scan-Informationen kann begrenzt werden. Der Standardwert ist 8 Ebenen. Darüber hinaus werden nur Informationen gespeichert, wenn sich diese von ihren Eltern unterscheiden. Sie können diese Einstellung verringern, um den Speicherverbrauch der CARO-Datenbank zu reduzieren.



Hinweis

Diese globale Einstellung der Scantiefe kann nachträglich angepasst werden bei der Einrichtung eines neuen Scans:



Beispiel für eine vollständige Speicherung

Scantiefeneinstellungen

Maximale Scantiefe

10

Legen Sie die maximale Ebene fest, bis zu der Scans und Analysen durchgeführt werden sollen.

Begrenzung der vollständigen Speicherung

8

Begrenzt die Ebenen für die vollständige Speicherung aller gesammelten Scan-Informationen. Darüber hinaus werden nur Informationen gespeichert, wenn sich diese von ihren Eltern unterscheiden. Sie können diese Einstellung verringern, um den Speicherverbrauch zu reduzieren.





Anzeige in der Ressourcen-Ansicht

Jede Ebene wird in der Ressourcenansicht im Baum angezeigt:

Icon	Name	Scan-Zeit	Auffälligkeiten hier	Auffälligkeiten unterhalb	Verteilung der Berechtigungen
→	C:\Users	15.6.2023, 14:23	!	!	
→	Test Marketing	15.6.2023, 14:23	!	!	
→	Department	15.6.2023, 14:23		!	
→	Marketing 1	15.6.2023, 14:23		!	
→	Raum 1	15.6.2023, 14:23	!	!	
→	Ebene 5	15.6.2023, 14:23		!	
Kinder von Ebene 5					
	Ebene 6	15.6.2023, 14:23	!		

Ressourceansicht mit Baumstruktur,
alle Ebenen sind aufgeklappt

Beispiel für eine Speicherbegrenzung

Die vollständige Speicherung ist begrenzt auf 2 Ebenen, es werden unterhalb der Ebene 2 nur Verzeichnisse mit geänderten Berechtigungen gespeichert und angezeigt:

Scantiefeneinstellungen

Maximale Scantiefe

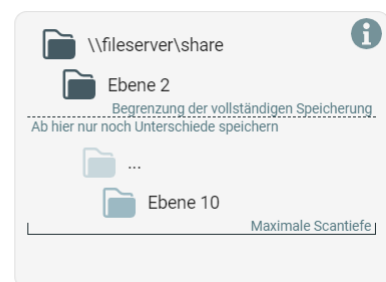
10

Legen Sie die maximale Ebene fest, bis zu der Scans und Analysen durchgeführt werden sollen.

Begrenzung der vollständigen Speicherung

2

Begrenzt die Ebenen für die vollständige Speicherung aller gesammelten Scan-Informationen. Darüber hinaus werden nur Informationen gespeichert, wenn sich diese von ihren Eltern unterscheiden. Sie können diese Einstellung verringern, um den Speicherverbrauch zu reduzieren.



Anzeige in der Ressourcen-Ansicht

In der Ressourcenansicht werden alle Verzeichnis-Ebenen „dazwischen“ nicht mehr im Baum angezeigt. Im Tooltip oder über ein Kästchen am untergeordneten Verzeichnis sehen Sie, in welcher Ebene wieder ein Verzeichnis mit geänderter Berechtigungslage existiert. Dies wird wie gewohnt im Baum angezeigt:

Icon	Name	Scan-Zeit	Auffälligkeiten hier	Auffälligkeiten unterhalb	Verteilung der Berechtigungen
→	C:\Users	15.6.2023, 10:41	!	!	
→	Test Marketing	15.6.2023, 10:41		!	
→	Raum 1	15.6.2023, 10:41	!	!	
Kinder von Raum 1					
	Ebene 6	15.6.2023, 10:41	!		

Ressourcenansicht, Ebene „Raum1“ und untergeordnete Kind-Elemente

Tooltip mit Details im untergeordneten Verzeichnis **Raum 1**:



Es gibt 2 übergeordnete Ebenen, die aufgrund der aktuellen Scantiefeneinstellung nicht gespeichert wurden:

- Raum 1
 - 1 Department
 - 2 Marketing 1
- Raum 1

Alle Ebenen oberhalb von **Ebene 6**:

Es gibt eine übergeordnete Ebene, die aufgrund der aktuellen Scantiefeneinstellung nicht gespeichert wurde:

- Raum 1
 - 1 Ebene 5
- Ebene 6

Übersicht

Nach dem Speichern sehen Sie in einer Liste Ihre konfigurierten Scan-Einstiegspunkte, sortiert nach Technologien. Wenn Sie alle Scan-Einstiegspunkte erfasst haben, ist die Grundkonfiguration abgeschlossen und wir können uns der Datenbereinigung widmen.

Active Directory Microsoft Entra ID Filesystem Lokale Konten Exchange Online						
Erstellen CARO hilft!						
Einstiegspunkte filtern...						
Name	Uri	System	Anmeldedaten	Verwendungszweck	Sonst. Einstellungen	
dev	\\dev	dev	cusatum\...	Bereinigung DB LIVE	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	
fileserver	\\fileserver	fileserver	cusatum\...	Bereinigung DB	Max. 8 Ebenen (4 vollst. speichern) Lokale Konten mitscannen	
Abteilungen (fileserver)	\\fileserver\Abteilungen	fileserver	cusatum\...	Bereinigung DB LIVE	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	
File-Server\$ (fileserver)	\\fileserver\File-Server\$	fileserver	cusatum\...	Bereinigung DB	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	
Finanz (fileserver)	\\fileserver\Finanz	fileserver	cusatum\...	Bereinigung DB LIVE	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	
GF (fileserver)	\\fileserver\GF	fileserver	cusatum\...	Bereinigung DB LIVE	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	
IT (fileserver)	\\fileserver\IT	fileserver	cusatum\...	Bereinigung DB LIVE	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	
Mein Marketing Einstiegspunkt	\\fileserver\Marketing	fileserver	cusatum\...	Bereinigung DB LIVE	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	
Personal (fileserver)	\\fileserver\Personal	fileserver	cusatum\...	Bereinigung DB LIVE	Max. 10 Ebenen (8 vollst. speichern) Lokale Konten mitscannen	

Liste von Einstiegspunkten für Filesystem



Hinweis

Wenn Sie als Einstiegspunkt einen **DFS-Share** konfigurieren wollen, bitte beachten Sie die Besonderheiten bei vererbten Berechtigungen mit NTFS-Freigaben und DFS. Viele Firmen setzen DFS ein. Die Ordnerziele sind meist Freigaben. Aber was passiert, wenn diese Freigaben NTFS-technisch vererbt, also alle Berechtigungen vom Elternverzeichnis erhalten sollen?

Sollten Sie Fragen dazu haben, bitte wenden Sie sich an unseren Support support@cusatum.de
Zum besseren Verständnis haben wir auf unserer Plattform in der Wissensdatenbank einen Eintrag hinterlegt:
<https://cusatum.de/dfs-probleme-mit-freigaben/>



Microsoft Entra ID Anbindung

App-Registrierung über integrierten Workflow

Für die Anbindung von CARO an ein Entra ID-System bieten wir Ihnen einen integrierten *4-Klick-Workflow* zur App-Registrierung ihres Client-Secrets an. Wo andere Hersteller oft nur eine Hilfestellung per Webseite anbieten, brauchen Sie bei CARO nur den Tenant-Namen des Entra ID-Systems einzugeben, der Registrierungsprozess wird anschließend automatisch durchgeführt.

Am Anfang wählen Sie bitte, ob Sie eine neue Anwendung registrieren müssen, oder ein bestehendes Client-Secret für die Anbindung von CARO an Ihren Entra ID-Tenant nutzen wollen.

Schritt 1: Auswahl eines Client-Secrets

Eine Anwendung neu registrieren über den 4-Klick-Workflow, Sie werden durch den Anmeldeprozess geführt. Hier Schritt 3 vor und nach der Registrierung:

Schritte 2 und 3: Autorisierung und Registrierung

Im letzten Schritt 4 wird die Anmeldung in die CARO-Konfiguration übernommen. Sie können nun einen Entra ID-Einstiegspunkt konfigurieren.

Active Directory Einstiegspunkte

Sie können als Einstiegspunkte auch Active Directory-Ressourcen zum Scannen auswählen. Bitte beachten Sie, dass Sie derzeit die Domäne als LDAP-Pfad konfigurieren müssen:



Domäne

Alternativ können Sie über die Schaltfläche **Durchsuchen** live Ihre Domäne suchen und auswählen.

Derzeit sind 73 Attribute konfigurierbar. Es werden 11 Objektklassen zum Scannen benutzt:

Objektklassen (11)

☐ user
 ☐ inetOrgPerson
 ☐ group
 ☐ computer
 ☐ contact
 ☐ foreignSecurityPrincipal
 ☐ container
 ☐ msExchSystemObjectsContainer
 ☐ organizationalUnit
 ☐ domainDNS
 ☐ builtinDomain

Berechtigungen auslesen

Definieren Sie, ob sie zusätzlich auch die Berechtigungen von Ous und Containern auslesen wollen.

Berechtigungen auslesen

☒ Organisationseinheiten und Container

Zusätzlich Auslesen der Berechtigungen für Domänen-DNS, Builtin-Domänen-Container, Organisationseinheiten (OUs) und Container



Hinweis: Eine doppelte Konfiguration von Domänen als Einstiegspunkte ist nicht möglich. Falls Sie dies trotzdem konfigurieren, wird die Speicherung einer doppelten Domäne mit einer Fehlermeldung abgebrochen. Der URL-Pfad der Domäne wird hier geprüft, ob er bereits verwendet wird. Mehrfachbenutzung von URL-Pfaden in den Einstiegspunkten für Fileserver ist jederzeit möglich.



Best Practice-Tipp: Es ist sinnvoll, mit dem Baustein **EBIS** oder **ARCA** einen wiederkehrenden Domänenscan einzurichten. EBIS scannt neben Ihren Kontendaten auch die Berechtigungssituation in Ihren OU-Strukturen. Mit ARCA werden die Kontodaten zusätzlich auf möglich Probleme analysiert. Lesen Sie mehr zu den verfügbaren Bausteinen und Best Practices zur Bereinigung im Kapitel **Analysieren und Bereinigen**.

AD-Security Events überwachen mit dem Observer

Für Active Directory Einstiegspunkte können Sie nun AD-Security-Events überwachen. Das dafür verwendete Modul **Observer** ist in der Vollversion der CARO-Suite enthalten, es muss nicht extra installiert werden.

Der Observer liest die Security-Events aus dem Microsoft Security Event Log aus. Das Auslesen wird in regelmäßigen Abständen durchgeführt. Die Ergebnisse werden in die CARO-Datenbank geschrieben. Die vom Observer aufgezeichneten Ereignisse können in der CARO-Suite im **Globalen Logbuch** eingesehen werden. Am Logbuch eines einzelnen Objekts, z.B. ein Benutzerkonto, sind die aufgezeichneten Ereignisse ebenfalls einsehbar.



Hinweis: Eine Anleitung mit der Beschreibung aller technischen Grundvoraussetzungen, die auf Ihren Domaincontrollern erfüllt sein müssen, damit der AD-Observer korrekt arbeiten kann, finden Sie hier: **CARO-AD-Observer Voraussetzungen für den Betrieb**

Standard-Einstellung für den Observer

Im Konfigurationsmanager unter **Globale Einstellungen** können Sie die Standard-Einstellung für alle Ihre Observer hinterlegen. Diese werden beim Neuerstellen eines AD-Einstiegspunktes übernommen.



Technologien
Active Directory
Observer

Global > Technologien > Active Directory

Observer

Ereigniskategoriefilter
Aktivieren oder Deaktivieren Sie die Ereignisse, die überwacht werden sollen. Diese Einstellung ist eine Standardeinstellung und wird bei einer Neukonfiguration übernommen.

Erstellen von Objekten, Löschen von Objekten, Ändern von Objekteigenschaften, Ändern von Gruppenmitglied...

Zu ignorierende Eventautoren
Definieren Sie eine Liste aller Eventautoren, deren Änderungen nicht überwacht werden sollen. Diese Einstellung ist eine Standardeinstellung und wird bei einer Neukonfiguration übernommen.

CUSATUM\Administrator

CUSATUM\Testadmin

Zu ignorierende Domänencontroller
Definieren Sie die Liste aller Domänencontroller, auf denen Änderungen nicht überwacht werden sollen. Mehrere sind mit ";" zu trennen. Zum Beispiel 'dc01.example.com,dc02.example.com'. Diese Einstellung ist eine Standardeinstellung und wird bei einer Neukonfiguration übernommen.

dc01.example.com

16 / 1024

Maximales Aktualisierungsintervall
Geben Sie die maximale Zeit in Sekunden an, die vergehen darf, bis die Eventlogs wieder vom Observer ausgelesen werden. Diese Einstellung ist eine Standardeinstellung und wird bei einer Neukonfiguration übernommen.

199

5 - 600

Zu ignorierende Objektklassen
Definieren Sie die Liste aller Objektklassen, die vom Observer ignoriert werden sollen. Mehrere Einträge sind mit ";" zu trennen. Zum Beispiel 'usergroup,computer'. Diese Einstellung ist eine Standardeinstellung und wird bei einer Neukonfiguration übernommen.

dnsNode,dnsZone,dnsZoneScope,dnsZoneScopeContainer,domainDNS,msDNS-ServerSettings

81 / 1024

Aufbewahrungstage für Observer-Events

Sie können definieren, wie lange die Observer-Events in der CARO-Datenbank aufbewahrt werden sollen.

Datenbank
Richtlinien zur Datenaufbewahrung
Dokumentation

Global > Datenbank > Richtlinien zur Datenaufbewahrung

Dokumentation

Observer-Aufbewahrungstage
Maximale Anzahl an Tagen, die Observer-Dokumentation gespeichert bleibt.

365

2 - 365

Observer-Konfiguration

Schalten Sie den Observer für AD-Einstiegspunkte ein:

Observer

☒ Aufzeichnen von Ereignissen

In der Tabgruppe „Observer“ finden Sie im Einstiegspunkte-Bearbeiten-Dialog alle Einstellungen für das Überwachen von Ereignissen.

▶ Scan

🔍 Observer ☒

Ereignis-Kategorien

Definieren Sie, welche Ereignisse aufgezeichnet werden sollen:

- Erstellen von Objekten, u.a. neue Gruppen oder Benutzer werden erzeugt
- Löschen von Objekten, u.a. Gruppen, Benutzer, Computer werden gelöscht
- Änderungen an Objekten, u.a. Attribut-Änderungen an Benutzer-Konten
- Änderungen an Gruppenmitgliedschaften
- Lokale Gruppenrichtlinienobjekt-Änderungen (local GPOs)
- Globale Gruppenrichtlinienobjekt-Änderungen (global GPOs)



Ereignisse aufzeichnen (4/6)

- ☒ Erstellen von Objekten
- ☒ Löschen von Objekten
- ☒ Änderungen an Objekten
- ☒ Gruppenmitgliedschafts-Änderungen
- ☐ Lokale Gruppenrichtlinienobjekt-Änderungen
- ☐ Globale Gruppenrichtlinienobjekt-Änderungen



Insgesamt gibt es 4 Observer-Ereignis-Kategorien, welche aufgezeichnet und im globalen Logbuch angezeigt werden.

Ausschluss-Liste von Domänencontrollern

Zu ignorierende Domänencontroller

Definieren Sie die Liste aller Domänencontroller, auf denen Änderungen nicht überwacht werden sollen. Mehrere sind mit ',' zu trennen. Zum Beispiel 'dc01.example.com,dc02.example.com'.

Definieren Sie hier eine Liste aller Domänencontroller, auf denen Änderungen nicht überwacht werden sollen. Mehrere sind mit ',' zu trennen. Zum Beispiel 'dc01.example.com,dc02.example.com'.

Ausschluss-Liste von Eventautoren

Definieren Sie hier eine Liste von Eventautoren, deren Änderungen nicht überwacht werden sollen.

Zu ignorierende Eventautoren (1)

Definieren Sie die Liste aller Eventautoren, deren Änderungen nicht überwacht werden sollen.

Maximales Aktualisierungsintervall

Geben Sie die maximale Zeit in Sekunden an, die vergehen darf, bis die Eventlogs wieder vom Observer ausgelesen werden.

Maximales Aktualisierungsintervall

Geben Sie die maximale Zeitspanne in Sekunden an, die vergehen darf, bevor der Observer die Ereignisprotokolle erneut liest.

Ausschluss-Liste für Objektklassen

Definieren Sie die Liste aller Objektklassen, die vom Observer ignoriert werden sollen. Mehrere Einträge sind mit ',' zu trennen. Zum Beispiel 'user,group,computer'. Diese Einstellung ist eine Standardeinstellung.

Zu ignorierende Objektklassen

Definieren Sie die Liste aller Objektklassen, die vom Observer ignoriert werden sollen. Mehrere Einträge sind mit ',' zu trennen. Zum Beispiel 'user,group,computer'. Diese Einstellung ist eine Standardeinstellung und wird bei einer Neukonfiguration übernommen.

81 / 1024

Attribut-Änderungen

Definieren Sie, welche Attributänderungen Sie beobachten wollen. Wählen Sie dazu aus der Liste der LDAP-Attribute Ihre Attribute aus, welche für Ihre Aufzeichnungen genutzt werden sollen. Diese Einstellung wird verwendet, wenn Sie bei Ereigniskategorie „Änderung an Objekten“ ausgewählt haben.

Zu beobachtende Attribut-Änderungen: 58



Konfigurieren

58

Es sind insgesamt 58 aufzuzeichnende LDAP-Attribute für den Observer konfiguriert. Sie können die Attribute ändern, indem Sie auf die Schaltfläche 'Konfigurieren' klicken.



Globale Einstellungen

Smart Permissions©

Smart Permissions steht für automatisch erzeugte Berechtigungsgruppen. Berechtigen Sie Ihre Benutzer über vordefinierte Regeln, welche Sie pro Einstiegspunkt oder Freigabe konfigurieren können. CARO erstellt dazu automatisch die passenden Berechtigungsgruppen oder nutzt vorhandene Gruppen. Sie können an jedem Einstiegspunkt bzw. jeder Freigabe die Regeln bestimmen, wie Ihre Berechtigungsgruppen erstellt werden sollen. Als Standard ist immer bereits der Scope **Global** definiert.

Definieren Sie die OU für die automatisch erstellten Berechtigungsgruppen:

Erstellen

Entfernen

Systemstandard

Layout

Filtern...

Alle Zuletzt bearbeitet

Scope ↑

Global

\\fileserv\Personal

OU für Berechtigungsgruppen

Definieren des Containers oder der OU, in dem die Berechtigungsgruppen erstellt werden.

Suche

Keine Einträge vorhanden

Der Wert ist nicht definiert.

Global

Einstellungen für Smart-Permissions

Smart-Permissions aktivieren

☒ Aktiviert die Benutzung von Smart-Permissions. Es werden automatisch Berechtigungsgruppen basierend auf den Zugriffsrechten erstellt und zugewiesen.

Automatische Gruppenerzeugung

Berechtigungsgruppen automatisch erzeugen

☒ Berechtigungsgruppen werden automatisch erstellt, wenn Zugriffsrechte zugewiesen werden, die eine Berechtigungsgruppe erfordern würden, die noch nicht existiert.

Gruppentyp

Der Gruppentyp wird für die automatisch erstellten Berechtigungsgruppen verwendet.

Lokal

OU für Berechtigungsgruppen

Definieren des Containers oder der OU, in dem die Berechtigungsgruppen erstellt werden.

Suche

Caro-Berechtigungsgruppen

OU=Caro-Berechtigungsgruppen,DC=cusatum,DC=de

Erstelle Unter-OU mit dem Server-Namen für Berechtigungsgruppen

☒ Neu erstellte Berechtigungsgruppen befinden sich in einer Unter-OU mit dem Servernamen, um das Active Directory übersichtlicher zu strukturieren.

Bildung des Gruppennamens - Kürzung des Verzeichnispfads

Der Verzeichnisname wird für die Bildung des Berechtigungsgruppennamens gekürzt. Es kann entweder der komplette Pfad oder ein Teil davon verwendet werden. Maximal sind 64 Zeichen erlaubt.

Systemnamen verwenden

☐ Der Name des Systems wird bei der Berechtigungsgruppennamensbildung genutzt.

Kompletten Pfad des Verzeichnisses verwenden

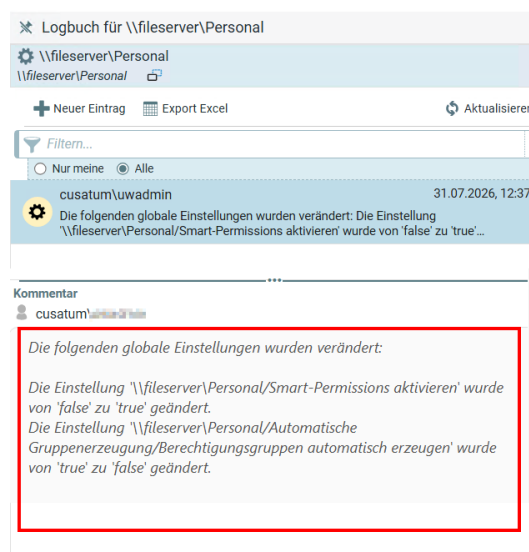
☒ Verwende den kompletten Pfad des Verzeichnisses für die Gruppennamensbildung. Wenn deaktiviert, wird nur ein Teil des Pfads verwendet, der durch den Index des ersten und letzten Verzeichnisses definiert ist.

Ihre Änderungen an einzelnen Konfigurationseinträgen werden protokolliert und können im Logbuch auf dieser View im rechten Seitenbereich (Sidepanel) und im Globalen Logbuch eingesehen werden.

 Logbuch
Seitenbereich

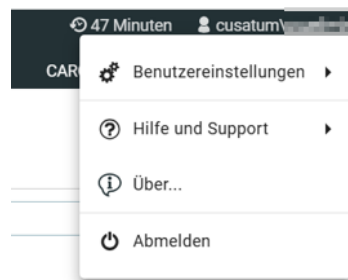
Seite 18/89

Smart Permissions©
Handbuch Version: 2026.9



Benutzereinstellungen

Das Menü für die Benutzereinstellungen wird durch Klick auf das Anmeldekonto im oberen Headerbereich der CARO-Suite geöffnet:

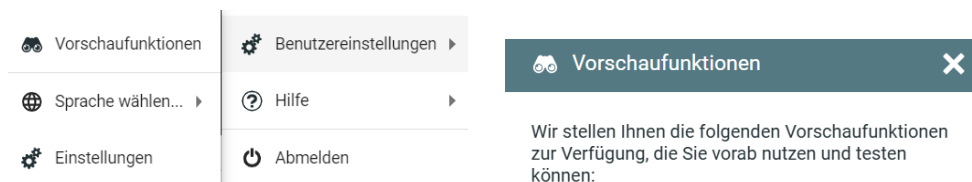


Sie können hier weitere Einstellungen vornehmen, Ihre Anzeigesprache anpassen, saisonale Motive für den Header der CARO-Suite definieren, sowie Vorschaufunktionen freischalten.

Saisonale Motive bedeutet, dass Sie je nach Jahreszeit den Headerbereich der CARO-Suite anders anzeigen lassen können. Im Herbst wird es ein Blätterrascheln geben, im Winter wird Ihre CARO-Suite Schneefall anzeigen. Lassen Sie sich überraschen, welche Motive es noch gibt!

Freischalten der Vorschaufeatures

In jedem Release gibt es einige Funktionen der CARO-Suite, welche als Preview-Funktionen bereits zur Verfügung stehen. Diese Vorschaufeatures müssen Sie im User-Menü unter **Benutzereinstellungen – Vorschaufunktionen** einmalig einschalten, falls Sie diese nutzen möchten.





Analysieren und Bereinigen

Mit der CARO-Suite können Sie umfangreiche Analysen und Bereinigungen durchführen. Die CARO-Suite enthält dazu **50 Risikoanalysen**, viele davon mit der Option einer automatisierten Bereinigung. Eigene Analysen können Sie schnell und einfach einbinden.

Funktionsübersicht

Funktion	Umsetzung
Risikobewertungs-Dashboard	
50 detaillierte Risikoanalysen mit integriertem Expertenwissen	
Kontenansicht Anzeige aller Gruppenmitgliedschaften, Kontensuche, auch über Attribute, Live-Kontensuche und Live-Ansicht.	
Graphische Darstellung von Konten- und Gruppenbeziehungen Anzeige von Konten-Beziehungen zur schnellen Visualisierung von Mehrfach-Zugriffen, auch indirekte Zugriffe werden dargestellt.	



Wo hat ein Benutzer/Gruppe Zugriff?

Ermitteln Sie mit einem Klick alle Ressourcen, auf die ein Konto Zugriff hat, auch über allgemeine Zugriffsgruppen.

2	Andern	Jeder
1	Andern	Authentifizierte Benutzer
2	Lesen & Ausführen	CUSATUM\Group 1
2	Andern	Jeder
2	Andern	Authentifizierte Benutzer
2	Andern	Authentifizierte Benutzer
2	Andern	Jeder

Berechtigungsansicht, Live-Ansicht

Berechtigungen überprüfen mit der Live-Ansicht, auch ohne Scan.

Besitzer	Verteilung der Berechtigungen
DEV-UTE\Administrator	100%
CUSATUM\Administrator	100%
fileserver\Administrators	100%
CUSATUM\Administrator	100%
CUSATUM\Administrator	100%
fileserver\Administrators	100%
fileserver\Administrators	100%

Überwachung von AD-Security-Ereignissen

Überwachung von ausgewählten AD-Security-Events, definieren der Attribute und Blacklist für Domain-Controller möglich. Ereignisse werden im Globalen Logbuch protokolliert.

Scan Observer

Ereignisse aufzeichnen (4/6)

- ☒ Gruppenmitgliedschafts-Änderungen
- ☒ Erstellen von Gruppen
- ☒ Löschen von Gruppen
- ☒ Attribut-Änderungen
- ☐ Lokale Gruppenrichtlinienobjekt-Änderungen
- ☐ Globale Gruppenrichtlinienobjekt-Änderungen

Ausgeschlossene Domänencontroller

dc01.example.com

Zu beobachtende Attribut-Änderungen (73)

Konfigurieren Zurücksetzen

73

Es sind insgesamt 73 aufzuzeichnende LDAP-Attribute für den Observer konfiguriert. Sie können die Attribute ändern, indem Sie auf die Schaltfläche 'Konfigurieren' klicken.

Insgesamt gibt es 4 Observer Ereignis-Kategorien, welche aufgezeichnet und im globalen Logbuch angezeigt werden.

Die Bereinigungsbausteine und ihre Anwendungsfälle

Die CARO-Suite umfasst derzeit 13 Analyse- und Bereinigungsbausteine mit insgesamt 50 einzelnen Analysen. Zusätzlich gibt es den Scan-Baustein EBIS zum Erfassen der IST-Situation Ihrer Systeme.

Die Bausteine werden bei der Konfiguration eines Scans bzw. beim Konfigurieren einer neuen Bereinigung angeboten. Für eine effiziente Grundbereinigung Ihrer IT-Systeme gibt es sinnvolle Kombinationen und eine empfohlene Reihenfolge für den Start der einzelnen Analysen.

Finden Sie alle Informationen zu den einzelnen Analysen und Bausteinen im PDF-Dokument: [CARO-Suite Analysieren und Bereinigen – Best Practises](#). Für einen optimalen Einsatz aller Analysen und Bereinigungen werden diese darin kurz erläutert mit praktischen Anwendungsfällen.

Risikoeinstufung der Analysen

Die erkannten Probleme aus den Analysen der CARO-Suite werden analog zur Risikobewertung zur BSI-Risikomatrix in 3 Kategorien eingestuft: kritische, wichtige und auffällige Probleme von Zugriffsrechten. (Quelle: Matrix zur Einstufung von Risiken, BSI-Standard 200-3, www.bsi.bund.de/grundschatz, v 1.0).



Risikobewertung	Erklärung
Kritisch	Kritische Fehler entstehen durch unzulässige Zugriffsrechte und sollten vorrangig beseitigt werden.
Wichtig	Analysen finden weitere als wichtig eingestufte Probleme in Ihrem System. Solche relevanten Probleme sollten zeitnah behoben werden.
Auffällig	Es werden Sicherheits-auffälligkeiten in den Zugriffsrechten gefunden. Diese Auffälligkeiten sollten nach unserer Erfahrung durch Ihre Administratoren überprüft werden.

Analysen mit Risikoeinstufung kritisch

Kategorie	Risiko	Beschreibung	Technologie
Inaktive Computer	Kritisch	Analysiere alle Computer, ob sie zu lange inaktiv waren.	Active Directory
Benutzer-Kennwort läuft nicht ab	Kritisch	Analysiere alle Benutzer mit nie ablaufenden Kennwörtern	Active Directory
Unterbrochene Vererbung	Kritisch	Sucht Ordner mit deaktivierter Vererbung.	Filesystem
Direkte Benutzerberechtigungen	Kritisch	Erkenne und analysiere direkte Benutzerzugriffsrechte.	Filesystem
Erlaubte Besitzer	Kritisch	Erlaubte Besitzer Analyse	Filesystem
Redundante Zugriffsrechte	Kritisch	Erkenne und analysiere redundante Zugriffsrechte für Konten.	Filesystem
Ablaufende Clientschlüssel	Kritisch	Analysiere alle Anwendungs-Registrierungen nach ablaufenden Clientschlüsseln.	Entra ID
Globale Administratoren	Kritisch	Analysiere alle Globalen Administratoren.	Entra ID
Globale Administrator-Rolle	Kritisch	Best Practices für die Anzahl an Globalen Administratoren.	Entra ID
Privilegierte Rollen	Kritisch	Best Practices für Anzahl an privilegierten Rollenzuweisungen.	Entra ID
Aktivierte Vererbung	Kritisch	Die Vererbung von NTFS-Zugriffsrechten auf Freigaben sollte deaktiviert sein. Das Ändern vererbter NTFS-Berechtigungen aus der Ferne löscht alle Zugriffsrechte und macht die Freigabe unbrauchbar.	Filesystem



Offene Freigabe	Kritisch	Alle authentifizierten Konten (Active Directory und lokal) haben mindestens das Lese-Zugriffsrecht auf die Informationen der Dateisystem-Freigabe. Damit kann ein unkontrollierter Datenabfluss erfolgen.	Filesystem
Nicht-administrative Laufwerks-Freigaben	Kritisch	Prüft auf nicht-administrative Freigaben mit Verweis auf komplette lokale Laufwerke.	Filesystem

Analysen mit Risikoeinstufung wichtig

Kategorie	Risiko	Beschreibung	Technologie
Inaktive Benutzer	Wichtig	Analysiere alle Benutzer, ob sie zu lange nicht angemeldet waren.	Active Directory
Ersteller-Besitzer	Wichtig	Entferne Ersteller-Besitzer-Berechtigungen.	Filesystem
Erforderliche Zugriffsrechte	Wichtig	Sicherstellen, dass Konten erforderliche Zugriffsrechte haben.	Filesystem
Verschobene Objekte	Wichtig	Erkenne und analysiere verschobene Objekte.	Filesystem
Zugriffsrechte ungewollter Konten	Wichtig	Prüfe bei allen Zugriffsberechtigungen, ob das berechtigte Konto eines der ungewollten Konten ist.	Filesystem
Inaktive Anwendungen	Wichtig	Analysiere alle Anwendungen, ob sie zu lange nicht angemeldet waren.	Entra ID
Inaktive Gast-Benutzer	Wichtig	Analysiere alle Gast-Benutzer, ob sie zu lange nicht angemeldet waren.	Entra ID
Cloud-Native Konten Rollenzuweisungen	Wichtig	Best Practices für die ausschließliche Nutzung von Cloud-Native Konten für Rollenzuweisungen.	Entra ID
Gruppen-Rollen-Zuweisungen	Wichtig	Best Practices für die ausschließliche Nutzung von Gruppen für Rollenzuweisungen.	Entra ID
Jeder Vollzugriff Freigabe	Wichtig	Das Jeder-Konto sollte maximal Ändern-Zugriffsrecht auf der Freigabe haben. Bei Vollzugriff besteht das Risiko, dass bei erweiterten NTFS-Zugriffsrechten Anwender unbewusst Schaden anrichten können.	Filesystem



List-Berechtigungen	Wichtig	Analyse aller Zugriffsberechtigungen von Verzeichnisbäumen hinsichtlich der Erreichbarkeit aller Verzeichnisse	Filesystem
---------------------	---------	--	------------

Analysen mit Risikoeinstufung auffällig

Kategorie	Risiko	Beschreibung	Technologie
Gruppen ohne Beschreibung	Auffällig	Alle Gruppen analysieren, die keine Beschreibung besitzen.	Active Directory
Leere Gruppen	Auffällig	Alle Gruppen analysieren, die keine Mitglieder besitzen.	Active Directory
Deaktivierte Benutzer	Auffällig	Analysiere alle Benutzer, die deaktiviert sind.	Active Directory
Deaktivierte Benutzer – x Tage inaktiv	Auffällig	Deaktivierte Benutzer, die mindestens x Tage nicht angemeldet waren.	Active Directory
Deaktivierte Benutzer in einer OU löschen	Auffällig	Überprüft alle Benutzer aus der konfigurierten OU, die deaktiviert sind und mindestens X Tage nicht geändert wurden.	Active Directory
Nie angemeldete Benutzer	Auffällig	Analysiere alle Benutzer, ob sie noch nie angemeldet waren.	Active Directory
Benutzer mit veraltetem Kennwort	Auffällig	Analysiere alle Benutzer, ob sie zu lange nicht ihr Kennwort verändert haben.	Active Directory
AD-Objekte mit RC4-Verschlüsselung	Auffällig	Alle Objekte mit RC4-Verschlüsselung analysieren (Rivest Cipher).	Active Directory
AD-Objekte mit KDC-Fallback auf Domänen-Standard	Auffällig	Alle Objekte mit KDC-Fallback auf Domänen-Standard analysieren (oft RC4).	Active Directory
Verwaiste Kontoreferenzen	Auffällig	Prüfe bei allen Zugriffsberechtigungen, ob das berechtigte Konto noch existiert.	Filesystem
Abgelaufene Client-schlüssel	Auffällig	Analysiere alle Anwendungs-Registrierungen nach abgelaufenen Clientschlüsseln.	Entra ID
Ablaufende Abonnements	Auffällig	Ablaufende Abonnements	Entra ID
Cloud-Native Benutzer	Auffällig	Analysiere alle Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.	Entra ID
Inaktive Cloud-Native Benutzer	Auffällig	Analysiere alle inaktiven Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.	Entra ID



Inaktive OnPrem-Benutzer	Auffällig	Analysiere alle inaktiven Benutzer, die mit einem On-Prem-AD synchronisiert sind.	Entra ID
Nicht-administrative Freigabe	Auffällig	Server auf die Existenz von Freigaben prüfen. Administrative Freigaben (C\$, etc.) werden ignoriert. Freigaben können unkontrollierten Zugriff auf kritische Informationen ermöglichen.	Filesystem
Austausch von Berechtigungen	Auffällig	Analyse der Berechtigung, um diese gegen ein gewünschtes Zugriffsrecht auszutauschen. Zur Vereinheitlichung für ein sauberes Berechtigungsmanagement-Konzept.	Filesystem
Freigegebene Postfächer	Auffällig	Analysiere alle freigegebenen Postfächer, denen keine Berechtigungen zugewiesen sind.	Exchange
Benutzer-postfächer	Auffällig	Analysiere alle Benutzerpostfächer, für die mehrere Konten Berechtigungen haben.	Exchange
Aktive Abwesenheits-notizen	Auffällig	Erkennt Postfächer mit aktivierter Out-of-Office-Konfiguration.	Exchange
Postfachgröße	Auffällig	Analysiere alle Postfächer, die eine bestimmte Größe überschreiten.	Exchange
Prüft CARO-Zugriffsgruppen	Auffällig	Prüft alle ACEs der CARO-Zugriffsgruppen	Filesystem
SID-Historie überprüfen	Auffällig	Prüfe alle ACEs, ob eine bestimmte Domänen-SID enthalten ist.	Filesystem
Verzeichnis-namenslänge	Auffällig	Prüft die Länge von Verzeichnisnamen.	Filesystem
Verzeichnis-pfadlänge	Auffällig	Prüft die Länge von Verzeichnispfaden.	Filesystem



Anpassung der Risikoeinstufungen

Die Risikoeinstufung für die einzelnen Analysen können Sie mit der CARO-Suite unter Globale Einstellungen an Ihre Vorgaben im Berechtigungsmanagement anpassen:

Parameter	Wert	Beschreibung
Inaktive Computer	Kritisch	Active Directory - Analysiere alle Computer, ob sie zu lange inaktiv waren.
Gruppen ohne Beschreibung	Auffällig	Active Directory - Alle Gruppen analysieren, die keine Beschreibung besitzen.
Leere Gruppen	Auffällig	Active Directory - Alle Gruppen analysieren, die keine Mitglieder besitzen.
Keine Member und keine Beschreibung	Auffällig	Keine Member und keine Beschreibung
Deaktivierte Benutzer	Auffällig	Active Directory - Analysiere alle Benutzer, die deaktiviert sind.
Deaktivierte Benutzer mit x Tagen inaktiv	Auffällig	Active Directory - Deaktivierte Benutzer, die mindestens x Tage nicht angemeldet waren.
Inaktive Benutzer	Wichtig	Active Directory - Analysiere alle Benutzer, ob sie zu lange nicht angemeldet waren.
Nie angemeldete Benutzer	Auffällig	Active Directory - Analysiere alle Benutzer, ob sie noch nie angemeldet waren.
Benutzer mit veraltetem Kennwort	Auffällig	Active Directory - Analysiere alle Benutzer, ob sie zu lange nicht ihr Kennwort verändert haben.
Benutzer Kennwort läuft nicht ab	Kritisch	Active Directory - Analysiere alle Benutzer mit nie ablaufenden Kennwörtern

Globale Konfiguration für Risiko-Kategorien für Analysen

Das CARO-Dashboard

Default-Dashboard

Auf der Home-Seite der CARO-Suite sehen Sie ein Dashboard. Dort werden verschiedene Widgets für die unterschiedlichen Aufgaben bereitgestellt. Auf der linken Seite befinden sich Widgets mit dem Fokus auf Bereinigungen und Risikobewertungen Ihrer gefundenen Berechtigungsprobleme. Auf der rechten Seite werden vorranging Status-Widgets angezeigt.

Nach der Erstinstallation und einem ersten Scan sehen Sie alle verfügbaren Widgets in einem Default-Dashboard.

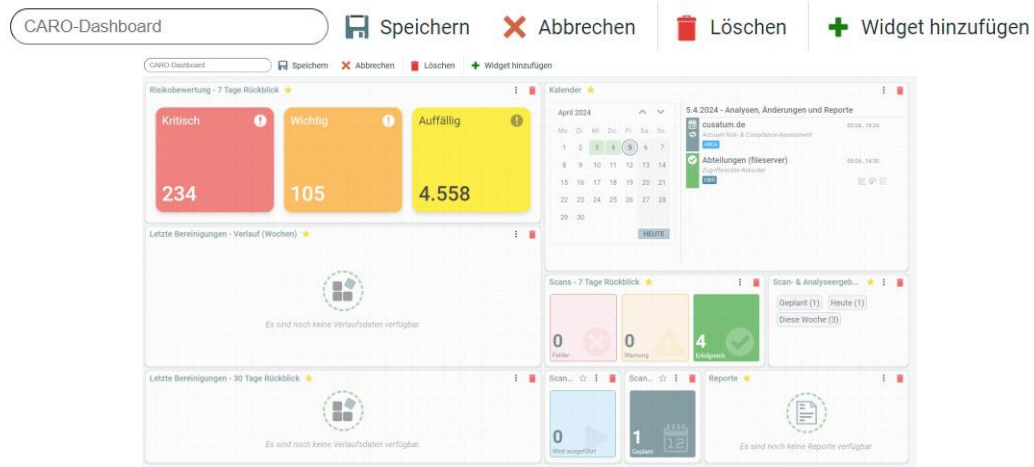
CARO-Dashboard auf der Home-Seite

Die Anordnung und Größe der Widgets können Sie selbständig ändern, d.h. Sie können neue Widgets hinzufügen, einzelne Widgets löschen oder die Position auf dem Dashboard verändern.

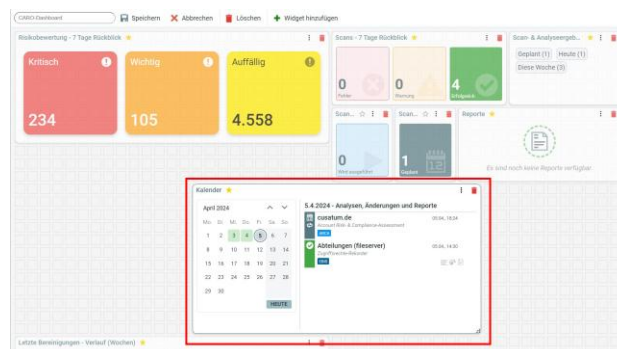


Dashboard bearbeiten

Über die Schaltfläche **Bearbeiten** wird der Bearbeiten-Modus Ihres aktuellen Dashboards aktiviert. Folgende Funktionen stehen dann in der Funktionsleiste zur Verfügung:



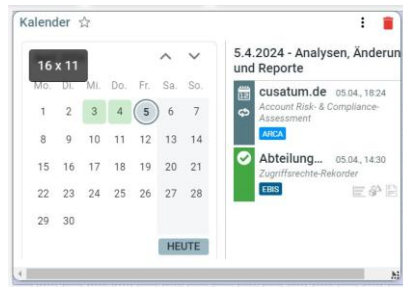
Die einzelnen Widgets sind nun verschiebbar oder löschar. Zum Verschieben einfach mit der Maus ein Widget „greifen“ bzw. anklicken und dann an die gewünschte neue Position verschieben. Die anderen Widgets positionieren sich automatisch in neue freie Flächen.



Hinweis: Bitte beachten Sie, dass die Dashboards eine feste Breite besitzen. Im Bearbeitungsmodus werden hierzu Gitternetzlinien als Orientierungshilfe angezeigt. Die Höhe eines Dashboards wird dagegen automatisch an die konfigurierten Widgets angepasst.

Widget-Größe ändern

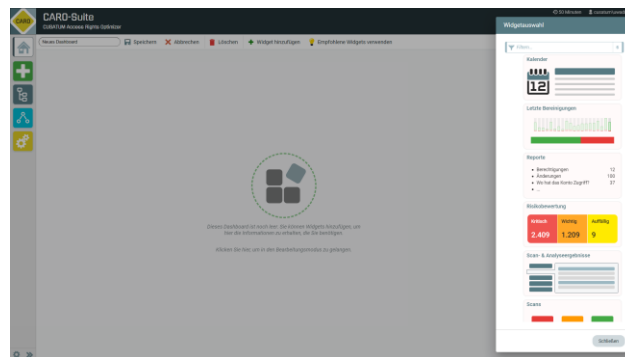
Sie können die Größe der einzelnen Widgets anpassen. Dazu in der rechten unteren Ecke mit der Maus einfach „ziehen“ und die Größe nach Ihren Wünschen verändern. In der dabei dunkel hinterlegten aktuellen Größen-Anzeige sehen Sie die aktuelle Breite und Höhe des Widgets **18 x 10**.



Haben Sie alle Widgets angeordnet, bzw. neue hinzugefügt oder entfernt, dann müssen Sie Ihr Dashboard abschließend noch speichern.

Ein neues Widget hinzufügen

Sie können beliebig viele Widgets auf Ihren Dashboards anordnen. Gehen sie dazu im Menü auf Widget hinzufügen, um die Seitenleiste mit allen verfügbaren Widgets anzuzeigen.



Anzeige der Seitenleiste zur Auswahl eines neuen Widgets

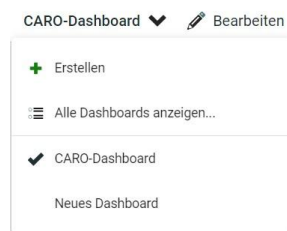
Wählen Sie Ihre gewünschten Widgets per Klick oder Benutzen Sie die Schaltfläche **Hinzufügen**.



Hinweis: Sie können mehrere Widgets mit der gleichen Funktionalität hinzufügen. In einem späteren Schritt können Sie die Inhalte eines Widgets mit Filtern an Ihre Bedürfnisse anpassen.

Ein neues Dashboard erzeugen

Sie können jederzeit ein neues Dashboard erstellen über das Menü **CARO-Dashboard**. Die Anzahl an Dashboards ist dabei nicht begrenzt.

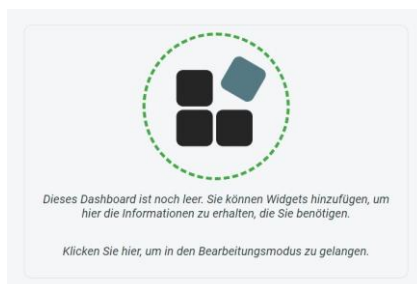




Initial wird nach dem Erstellen ein leeres Dashboard angezeigt. Durch Klick in die Mitte des leeren Dashboards oder über **Widget hinzufügen** wird die Seitenleiste mit den verfügbaren Widgets geöffnet. Alternativ können Sie über die Funktion

Empfohlene Widgets verwenden

das neue Dashboard mit Default-Widgets füllen. Durch Speichern wird ihr Dashboard in der CARO-Datenbank abgespeichert.



Einen Überblick über Ihre Dashboards erhalten Sie über die Funktion **Alle Dashboards anzeigen**. Sehen Sie, wann Sie Ihre Dashboards das letzte Mal bearbeitet oder verwendet haben. Die Anzahl der Widgets wird ebenfalls in der Übersicht angezeigt.

Wählen Sie ein Dashboard oder erstellen Sie ein neues				
+ Neues Dashboard erstellen 🗑 Löschen				
Name	Widgets	Erstellt	Zuletzt bearbeitet	Zuletzt verwendet
CARO-Dashboard	8	4.4.2024	Heute, 17:44 Vor 2 Stunden	Heute, 19:42 Gerade eben
Neues Dashboard	1	4.4.2024	4.4.2024 Vor 23 Stunden	Heute, 19:35 Vor 7 Minuten

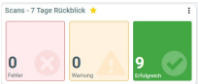
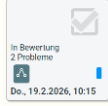
Liste aller konfigurierten Dashboards

Die Widgets und ihre Funktion

CARO bietet Widgets für die verschiedenen Aufgaben rund um die Bereinigung Ihrer Zugriffsrechte an.

Widget	Name	Gruppe	Wofür ist dieses Widget?
	<u>Widget Risikobewertung</u>	Analyse und Risk Assessment	Analyse der Berechtigungsprobleme, sortiert nach gescanntem System, filterbar nach Zeit
	<u>Widget Letzte Bereinigungen</u>	Fortschritt der Bereinigungen	Anzeige aller Bereinigungen über einen zeitlichen Verlauf von Tagen oder Wochen, Filterung nach einzelnen gescannten Systemen möglich



	<u>Widget Kalender</u>	Status und Aufgabenplanung	Anzeige aller Scans im Kalendermodus, Wann findet der nächste geplante Scan statt, Filterung nach Scans, Änderungen oder Reporten möglich
	<u>Widget Aufgaben</u>	Status aller Aufgaben	Anzeige von Scans, Reporten oder Verwaltungsaufgaben, gefiltert nach deren Status, erfolgreich ausgeführt, mit Warnungen oder mit Fehlern
	<u>Widget Arbeit fortsetzen</u>	Fortschritt der Bereinigungen	Die letzten Bereinigungen werden angezeigt und können fortgesetzt werden
	<u>Widget Verwaltungsaufgaben</u>	Verwalten	Überblick aller Aktionen, die mit CARO durchgeführt wurden oder geplant sind
	Reporte	Reporte	Alle mit CARO erstellten Reporte werden in einer Übersicht angezeigt
	Scan- und Analyseergebnisse	Status der Scans	Alte Home-Ansicht der CARO-Suite zur kompakten Darstellung aller Scans, sortiert nach Datum
	<u>Widget Globales Logbuch</u>	Verwalten	Überblick über alle durchgeführten Änderungen und erfassten Events durch den Observer

[Widget Risikobewertung](#)

Alle Analyseergebnisse von Berechtigungsfehlern bzw. -auffälligkeiten in Zugriffsrechten werden in die 3 Risikogruppen einsortiert und in diesem Widget angezeigt. Für diese Ansicht können Sie zeitliche Filter setzen:

- Heute
- Gestern und Heute
- 7 Tage Rückblick
- 14 Tage Rückblick
- 30 Tage Rückblick

Nach Klick auf das Widget öffnet sich die Detailansicht mit einer tabellarischen Anzeige aller Systeme, wo im gewählten Zeitbereich Berechtigungsprobleme gefunden wurden.





Detailansicht

Risikobewertung - 7 Tage Rückblick ★ Favoriten			
Übersicht			
Name	Kritisch	Wichtig	Auffällig
cusaturn	342	156	6.837
fileserver	6	1	0

Nach Auswahl einer Zeile in der Tabelle öffnet sich die Liste aller dazugehörigen Analysen für das gewählte System. Sie können hier Ihre Bereinigung starten, indem Sie alle oder einzelne Analysen auswählen und dann die Schaltfläche **Probleme bewerten** anwählen.



Hinweis: In der Detailansicht für ein System werden nur für einen begrenzten Zeitraum die Details und Analysen angezeigt. Ein Tooltip zeigt die aktuell konfigurierten Aufbewahrungstage an. Die aufsummierten Risikozahlen im Widget selbst (die großen Kacheln) gelten über alle Analysen, welche die CARO-Suite durchgeführt hat.

Aufgrund Ihrer aktuellen Aufbewahrungseinstellungen sind detaillierte Informationen nur für die letzten 28 Tage verfügbar.

- Datenbank > Richtlinien zur Datenaufbewahrung > Analyse-Ergebnisse
Aufbewahrungstage: 28 days

Widget Aufgaben

Im Widget Scans können Sie alle Informationen zur Ausführung und Konfiguration Ihrer Scans einsehen.





Detailansicht

Widget Kalender

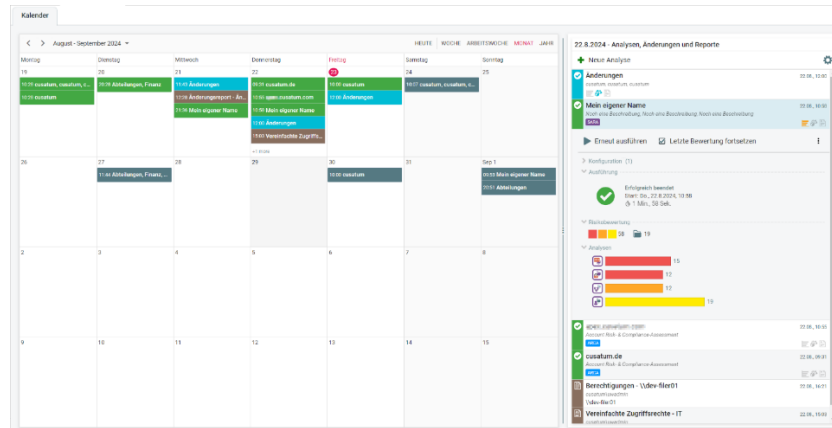
Im Widget Kalender werden alle Analysen, Änderungen oder Reporte zeitlich einsortiert und angezeigt. So haben Sie sofort einen Überblick, an welchen Tagen Ihre Analysen liefen, oder wann Sie Änderungen vorgenommen haben. Sie können den Anzeigemodus dieses Widgets festlegen über das Widget-Menü:

- Heute
- Kalender und Liste
- Kalender.

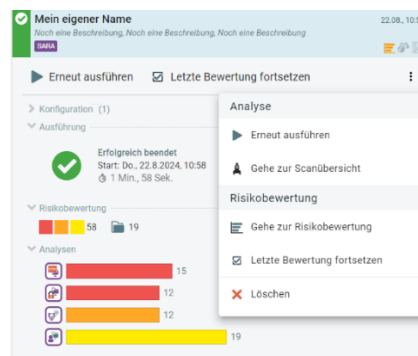
Oder Sie setzen den Anzeigefilter für Ihre Aufgaben:

Detailansicht

In der Detailansicht können Sie wählen zwischen verschiedenen Ansichten. Die Auswahl eines bestimmten Tages im Kalender aktualisiert die Liste auf der rechten Seite.



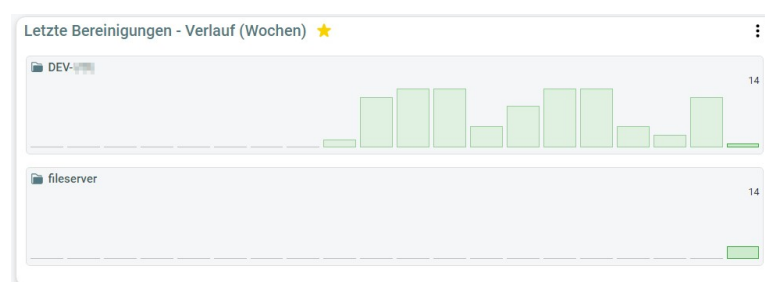
Für jede Aufgabe (Analyse, Änderung, Verwaltungsaufgabe oder Report) können Sie über ein Kontextmenü Funktionen ausführen. In diesem Beispiel wurde eine Analyse gewählt, welche bereits eine Bewertung beinhaltet. Über **Letzte Bewertung fortsetzen** kann man direkt zum Risiko-Dashboard navigieren.



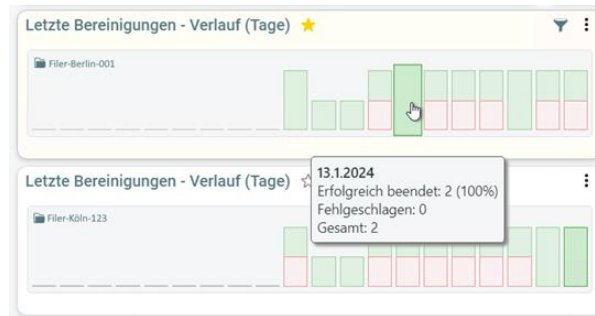
Widget Letzte Bereinigungen

Verlauf

Sehen Sie in dieser Ansicht den zeitlichen Verlauf Ihrer Bereinigungen, wann und auf welchen System Änderungen durchgeführt wurden. Ein Balken steht dabei für einen Tage, 1 Woche oder 1 Monat.

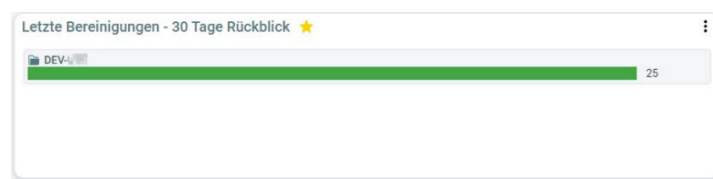


Wurden für Bereinigungen einzelne Änderungen nicht ausgeführt, wird CARO diese Rot markieren:



Rückblick

Der Anzeigemodus Rückblick werden alle Änderungen bzw. Bereinigungen für einen bestimmten Zeitbereich zusammengefasst.

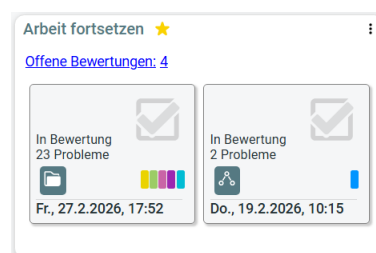


Folgende Filter sind möglich:

- Heute
- Gestern und Heute
- 7 Tage Rückblick
- 14 Tage Rückblick
- 30 Tage Rückblick

Widget Arbeit fortsetzen

Sie können hier Ihre noch offenen Bewertungen einsehen und einfach fortsetzen. Die letzten Bewertungen werden in einer Kachel im Widget auf dem Dashboard angezeigt. Wenn Sie weitere offene Bewertungen haben, können Sie diese in der Detailansicht sehen.



Detailansicht

Für alle offenen Bewertungen sehen Sie weitere Detailinformationen, z.B. auf welchem Verzeichnis oder in welcher OU wurden Berechtigungsprobleme gefunden. Ebenfalls sind der Autor und das Bearbeitungsdatum aufgeführt. Wenn Ihre Bewertung schon einige Zeit zurück liegt, kann es vorkommen, dass die passende Analyse dazu nicht mehr im System hinterlegt ist. Die Bewertung kann dann nicht mehr fortgesetzt werden und gilt als verwaist.



Arbeit fortsetzen
★ Favoriten

Fortsetzen
Verwerfen

Alle
Nur meine

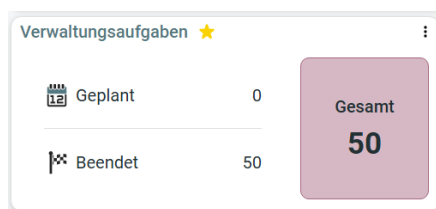
Aufgabe
Filter (4 Bewertungen)

Es gibt verwaiste Bewertungen, die aufgrund fehlender oder veralteter Informationen nicht mehr fortgesetzt werden können. Sie können ohne Bedenken gelöscht werden.

Status	Ressourcen	Information	Analysen	Erstellt	Autor
☒	Abteilungen (fileserv) \\fileserv\Abteilungen	23 Probleme bereits ausgewählt	BAPS DARS DUKE ERBE TEUS	Fr., 27.2.2026, 17:52	cusatum
☒	cusatum.de LDAP://DC=cusatum,DC=de	2 Probleme bereits ausgewählt	ARCA	Do., 19.2.2026, 10:15	cusatum
☒	Abteilungen (fileserv)	1 Problem bereits ausgewählt	ARCA	Sa., 31.1.2026, 13:20	cusatum
	Diese Bewertung ist verwaist und kann nicht mehr fortgesetzt werden.	0 Probleme bereits ausgewählt	Nicht verfügbar	Fr., 23.1.2026, 11:06	cusatum

Widget Verwaltungsaufgaben

Dieses Widget dient der schnellen Übersicht für Ihre durchgeführten und geplanten Verwaltungsaufgaben. Es ist nicht zu verwechseln mit den Logbuch-Einträgen, wo alle Änderungen protokolliert werden, welche CARO an Konten, Containern, Verzeichnissen oder anderen Objekten vorgenommen hat.



Hinweis: Die Information über Verwaltungsaufgaben wird nach einem bestimmten Zeitraum aus der Datenbank der CARO-Suite durch einen Maintenance-Job gelöscht. D.h. Ihre Verwaltungsaufgaben werden nach einer bestimmten Zeit aus der CARO-DB entfernt. Der Standardwert ist 60 Tage, er kann aber in der globalen Konfiguration angepasst werden.

Global > Datenbank > Richtlinien zur Datenaufbewahrung

Aufgabenausführungen

⚙️
Aufbewahrungstage
🕒

Maximale Anzahl an Tagen, die Aufgabenausführungen gespeichert werden.

168

2 - 168

Details

Sehen Sie alle aktuell gespeicherten Verwaltungsaufgaben auf einem Blick. Sie können nach bestimmten Aktionen suchen oder über die Filterfunktion bestimmte Objekte suchen, wo Sie Änderungen durchgeführt haben.



The screenshot shows the 'Verwaltungsaufgaben' (Management Tasks) widget. On the left, there's a sidebar with a list of tasks and their counts: 'Berechtigung entfernen' (1), 'Berechtigung hinzufügen' (12), 'Besitzer ändern' (4), 'Konto aktivieren' (1), 'Konto deaktivieren' (5), 'Konto löschen' (2), 'Kontomitgliedschaften ändern' (18), 'Neue Gruppe erzeugen' (2), and 'Ordner erstellen' (3). The main area displays a list of tasks, including 'Berechtigung hinzufügen' (Add Permission) and 'Berechtigung entfernen' (Remove Permission). A detailed view of a selected task is shown on the right, titled 'Selektierte Verwaltungsaufgabe'.

Haben Sie eine durchgeführte Änderung selektiert, können Sie sich die Details auf der rechten Seite anzeigen lassen. Navigieren Sie einfach zum geänderten Konto:

The screenshot shows the 'Selektierte Verwaltungsaufgabe' (Selected Management Task) window. It displays details for a task titled 'Konto-Mitglied' (Account Member). The task is marked as 'Gehe zur Kontenansicht' (Go to Account View). The window shows a list of parameters and values, including 'Gruppenmitglieder ändern' (Change Group Members), 'Mitglieder hinzufügen' (Add Members), 'Mitglieder entfernen' (Remove Members), 'Kommentar' (Comment), 'Gruppenmitgliedschaften ändern' (Change Group Memberships), 'Mitgliedschaften hinzufügen' (Add Memberships), 'Mitgliedschaften entfernen' (Remove Memberships), and 'Konto' (Account).

Widget Globales Logbuch

Alle Änderungen werden im Globalen Logbuch zentral dokumentiert und sind jederzeit nachvollziehbar. Im Widget sehen Sie eine Gesamtanzahl aller Änderungen und Ereignisse pro Ereignis-Quellentyp, die im konfigurierten Zeitraum, hier 30 Tage Rückblick, aufgetreten sind.

The screenshot shows the 'Globales Logbuch - 30 Tage Rückblick' (Global Logbook - 30 Day Review) widget. It displays a summary of events over the last 30 days. The widget shows counts for various event types: '1 Bereinigungen' (1 Cleanups), '25 Verwalten' (25 Manage), '39 Konfiguration' (39 Configuration), '23.818 Observer' (23,818 Observer), and '1 Manuell' (1 Manual).



Das Logbuch unterstützt unterschiedliche Quellen für Ereignisse. Durch Klick auf ein Kästchen einer Quellenart, z.B. „Bereinigungen“, wird das globale Logbuch vorgefiltert geöffnet.

The screenshot shows the 'Globales Logbuch' (Global Logbook) interface. At the top, there are several widgets: '23.885 Alle aus', '1 Bereinigungen' (highlighted with a red box), '25 Verwalten', '39 Konfiguration', '23.818 Observer', and '1 Manuell'. Below these, there are filters for 'Heute', '30 Tage Rückblick', and a date range '18.8.2026 - 17.9.2026'. A search bar is present with the text 'Suche'. The main content area shows a list of events, with the first event being 'cusatum\...'. The right sidebar shows 'Durchgeführte Aktionen' (Actions performed) and 'Ressourcen' (Resources).

Details

Mit dem Globalen Logbuch erhalten Sie eine schnelle Übersicht, welche Änderungen an Ihrem System vorgenommen wurden. Filter nach Quellen, Zeitraum, Autor, Konto- oder Verzeichnis-Namen sowie einer bestimmten Ticket-ID sind möglich.

The screenshot shows a detailed view of an event in the 'Globales Logbuch'. The 'Bereinigungen' widget is highlighted with a red box. The event details show 'Ändere Attribut 'accountExpires'' and 'Füge Attribut 'title' mit neuem Wert 'Herr Dr.' hinzu.' (Add attribute 'title' with new value 'Herr Dr.'). The right sidebar shows 'Durchgeführte Aktionen' (Actions performed) and 'Ressourcen' (Resources).

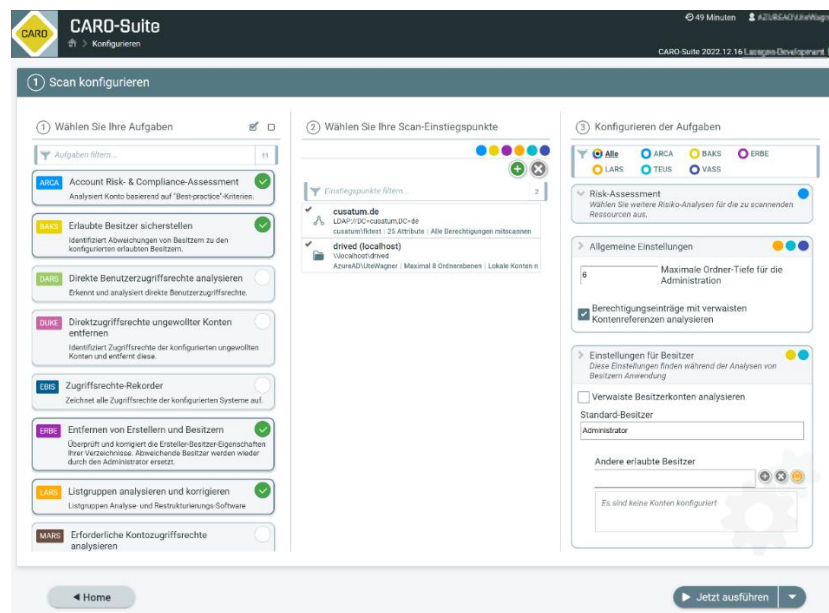
Im Kapitel [Globales Logbuch](#) finden Sie einen Funktionsüberblick, u.a. eine genaue Beschreibung über die Filtermöglichkeiten, welche Events kommen aus welchen Quellen, sowie weitere wichtige Funktionsbeschreibungen.



Neue Bereinigung: In 5 Schritten Ihr System bereinigen

Schritt 1: Einen Scan konfigurieren

Im ersten Schritt konfigurieren Sie Ihren Scan und die Analysemethoden. Wählen Sie zuerst die Bereinigungsbausteine aus, was CARO analysieren und bereinigen soll (linke Seite). Als Nächstes wählen Sie den Ort, wo gescannt und analysiert werden soll: das sind die **Scan-Einstiegspunkte**. Sie können hier mehrere Einstiegspunkte gleichzeitig zum Scan nutzen. Abschließend konfigurieren Sie noch zusätzliche Parameter, wie z.B. den Standardbesitzer, der nach der Analyse beim Bereinigen wieder gesetzt werden soll.



Hinweis: Bei einigen Analysen, z.B. für **EBIS**, müssen nur die Einstiegspunkte konfiguriert werden. Weitere Einstellungen neben Scan-Einstellungen sind nicht notwendig.

Solange Sie eine unvollständige Konfiguration haben, können Sie keinen Scan starten. Einen entsprechenden Hinweis sehen Sie im unteren Bereich:



Wenn Sie Ihre Bausteine für die Analysen, die Einstiegspunkte zum Scannen und die notwendigen Parameter konfiguriert haben, wählen Sie abschließend aus, wann Sie Ihre Analyse starten wollen:

- sofort ausführen
- jetzt im Hintergrund ausführen
- heute Nacht oder
- an einem geplanten Zeitpunkt in der Zukunft. Sie können hier den Scan auch zeitgesteuert oder wiederkehrend planen und ausführen.



Best Practice-Tipp: Falls Sie eine Listgruppenanalyse mit dem Baustein **LARS** durchführen möchten, beachten Sie bitte, diesen Scan ausschließlich mit LARS zu starten. Andere Analysen sollten Sie separat ausführen. Sie können dafür weiterhin den gleichen Scan-Einstiegspunkt nutzen. Bei gleichzeitiger Nutzung von LARS mit



anderen Analyse-Bausteinen wird CARO zusätzlich verlangsamt, es kann zu unnötig langen Scan- und Analysezeiten kommen.

Konfiguration für ARCA

ARCA

Für Ihre Kontenanalysen können Sie das Modul **ARCA** nutzen. CARO bietet dazu verschiedene Analysen für unterschiedliche Technologien an. Nach der Auswahl Ihres Einstiegspunktes erhalten Sie eine gefilterte Ansicht pro Technologie der auswählbaren Risiko-Analysen.

Analysen für Active Directory (13)

▼ **Konten Risk-Assessment**
Wählen Sie weitere Risiko-Analysen für die zu scannenden Konten aus.

Risiko-Analysen für Konten (13/13)  

- ☒ **AD-Objekte mit KDC-Fallback auf Domänen-Standard**
Active Directory - Alle Objekte mit KDC-Fallback auf Domänen-Standard analysieren (oft RC4).
- ☒ **AD-Objekte mit RC4-Verschlüsselung**
Active Directory - Alle Objekte mit RC4-Verschlüsselung analysieren (Rivest Cipher).
- ☒ **Deaktivierte Benutzer in einer OU löschen**
Überprüft alle Benutzer aus der konfigurierten OU, die deaktiviert sind und mindestens X Tage nicht geändert wurden.
- ☒ **Leere Gruppen**
Active Directory - Alle Gruppen analysieren, die keine Mitglieder besitzen.
- ☒ **Gruppen ohne Beschreibung**
Active Directory - Alle Gruppen analysieren, die keine Beschreibung besitzen.
- ☒ **Inaktive Computer**
Active Directory - Analysiere alle Computer, ob sie zu lange inaktiv waren.
- ☒ **Keine Member und keine Beschreibung**
Keine Member und keine Beschreibung
- ☒ **Inaktive Benutzer**
Active Directory - Analysiere alle Benutzer, ob sie zu lange nicht angemeldet waren.
- ☒ **Nie angemeldete Benutzer**
Active Directory - Analysiere alle Benutzer, ob sie noch nie angemeldet waren.
- ☒ **Benutzer-Kennwort läuft nicht ab**
Active Directory - Analysiere alle Benutzer mit nie ablaufenden Kennwörtern
- ☒ **Deaktivierte Benutzer**
Active Directory - Analysiere alle Benutzer, die deaktiviert sind.
- ☒ **Deaktivierte Benutzer - x Tage inaktiv**
Active Directory - Deaktivierte Benutzer, die mindestens x Tage nicht angemeldet waren.
- ☒ **Benutzer mit veraltetem Kennwort**
Active Directory - Analysiere alle Benutzer, ob sie zu lange nicht ihr Kennwort verändert haben.



Analysen für Entra ID (13)

Konten Risk-Assessment
Wählen Sie weitere Risiko-Analysen für die zu scannenden Konten aus.

Risiko-Analysen für Konten (13/13)

- ☒ **Inaktive Anwendungen**
Entra ID - Analysiere alle Anwendungen, ob sie zu lange nicht angemeldet waren.
- ☒ **Cloud-Native Konten Rollenzuweisungen**
Entra ID - Best Practices für die ausschließliche Nutzung von Cloud-Native Konten für Rollenzuweisungen.
- ☒ **Cloud-Native Benutzer**
Entra ID - Analysiere alle Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.
- ☒ **Abgelaufene Clientschlüssel**
Entra ID - Analysiere alle Anwendungs-Registrierungen nach abgelaufenen Clientschlüsseln.
- ☒ **Ablaufende Clientschlüssel**
Entra ID - Analysiere alle Anwendungs-Registrierungen nach ablaufenden Clientschlüsseln.
- ☒ **Ablaufende Abonnements**
Entra ID - Ablaufende Abonnements
- ☒ **Globale Administrator-Rolle**
Entra ID - Best Practices für die Anzahl an Globalen Administratoren.
- ☒ **Globale Administratoren**
Entra ID - Analysiere alle Globalen Administratoren.
- ☒ **Gruppen-Rollenzuweisungen**
Entra ID - Best Practices für die ausschließliche Nutzung von Gruppen für Rollenzuweisungen.
- ☒ **Inaktive Gast-Benutzer**
Entra ID - Analysiere alle Gast-Benutzer, ob sie zu lange nicht angemeldet waren.
- ☒ **Inaktive Cloud-Native Benutzer**
Entra ID - Analysiere alle inaktiven Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.
- ☒ **Inaktive OnPrem-Benutzer**
Entra ID - Analysiere alle inaktiven Benutzer, die mit einem On-Prem-AD synchronisiert sind.
- ☒ **Privilegierte Rollen**
Entra ID - Best Practices für Anzahl an privilegierten Rollenzuweisungen.

Für einige Analysen können Sie zusätzliche Einstellungen für den Analyse- oder Bereinigungsprozess vornehmen:

Konfiguration für das Risk-Assessment von Konten
Zusätzliche Einstellungen für die Risk-Assessments von Konten.

LDAP-Pfad für deaktivierte Benutzer
Verschiebe alle deaktivierten Benutzer in diese OU

Maximale Anzahl an Tagen, die ein Benutzer nicht angemeldet war
1 – 9.999

Maximale Anzahl an Tagen, die ein Computer nicht angemeldet war
1 – 9.999

Maximales Password-Alter in Tagen
1 – 9.999

In der Bewerten-Ansicht, nach erfolgreicher Analyse sehen Sie zusätzliche Details:

Inaktive Benutzer 1 Hinweis

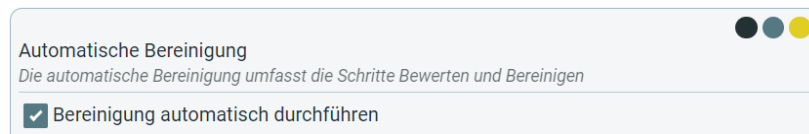
Hinweis

- Inaktiv seit mehr als 30 Tagen. Letzte Logon-Zeit war 27.07.2022 12:51:54.



Automatische Bereinigung

Sie können die Bereinigungen auch automatisch durchführen lassen. Dadurch werden Ihre Prozesse automatisiert, eine manuelle Überprüfung ist nicht notwendig.

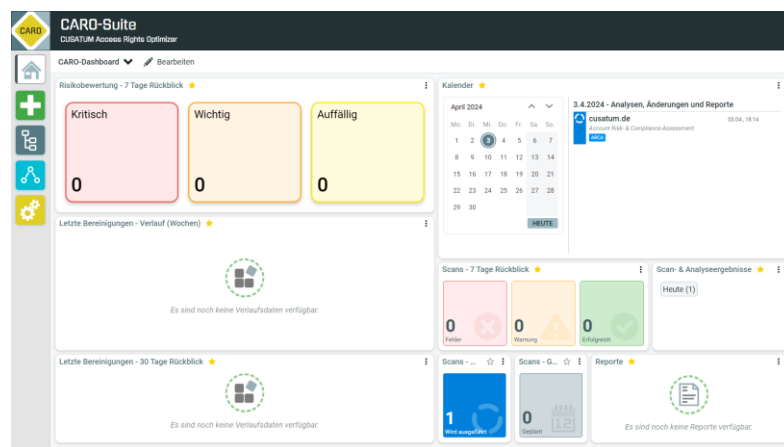


Weitere Details zu diesem Modus lesen Sie bitte im Kapitel [Automatisches Bereinigen mit der CARO-Suite](#).

Schritt 2: Risikobewertung und Analyse

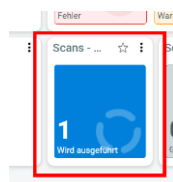
Risikobewertung

Nach dem Start Ihres Scans können Sie zum Home-Screen der CARO-Suite zurückkehren. Sie sehen hier das Dashboard der CARO-Suite.

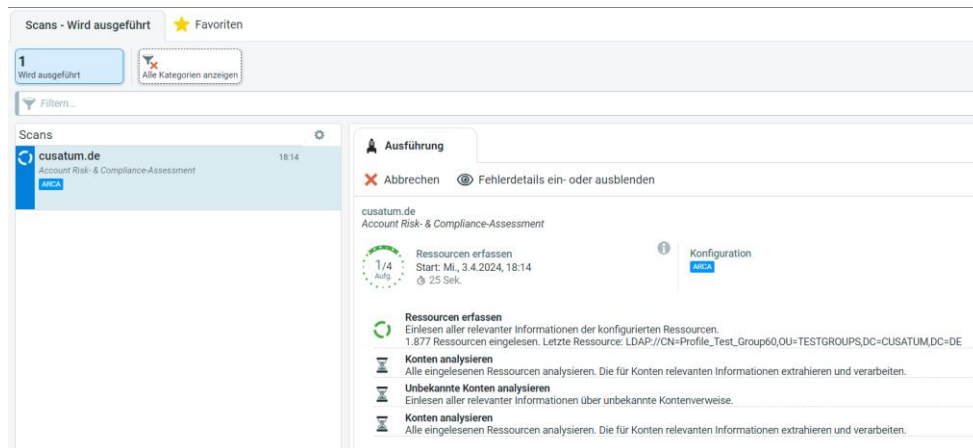


Das Dashboard ist dabei in Widgets aufgeteilt, wobei im linken Bereich die Risikobewertung und Bereinigungen im Fokus stehen. Auf der rechten Seite sind die Status-Informationen der Scans und Aufgaben zu finden. Sie können sich eigene Dashboards konfigurieren, um den Fokus auf Ihre jeweiligen Aufgaben zu legen. Sie können pro Widget verschiedene Filter über Zeit- oder gescannte Systeme setzen. Näheres dazu im Kapitel

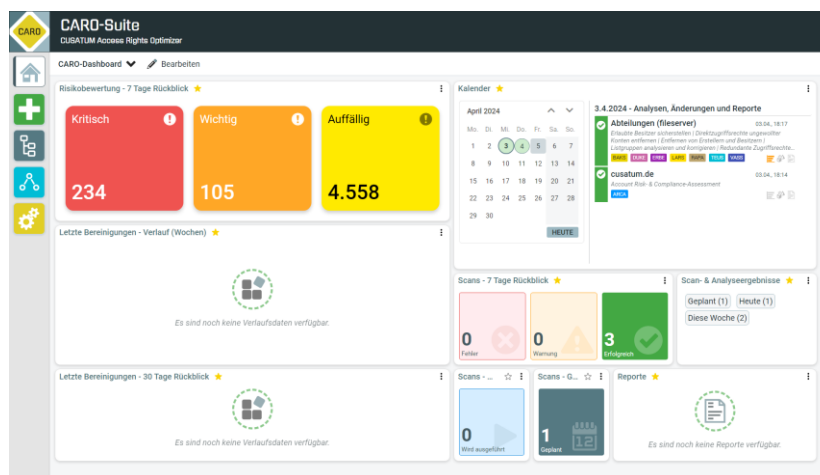
Das CARO-Dashboard.



Die Widgets können direkt mit der Maus angewählt werden. Man gelangt dann in die jeweilige Detailansicht eines Widgets. Zur Anzeige des ersten Scans klicken Sie einfach das Scan-Widget für **Wird ausgeführt-Scans** an. Danach öffnet sich diese Detailansicht:

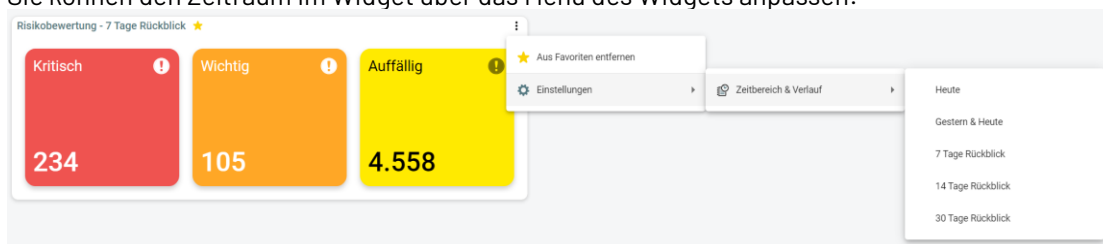


Nach Durchführung Ihrer ersten Scans für Filesystem und Active Directory finden Sie im Dashboard automatisch Ihre ersten Risikobewertungen auf der linken Seite im Widget **Risikobewertung**.



Die Risiko-Bewertung ist sortiert nach den gescannten Systemen und nach Risikogruppen. Dadurch erkennen Sie auf einen Blick, wo genau bei Ihnen die größten Risiken zu finden sind.

Sie können den Zeitraum im Widget über das Menü des Widgets anpassen:



Wenn Sie z.B. nur den Zeitraum Heute einstellen, wird die Risikobewertung entsprechend angepasst:





Zuordnung der Analysen zu Risiken

CARO führt für jede Analyse eine Risikobewertung durch und sortiert die gefundenen Fehler in die drei Risikogruppen ein: kritisch, wichtig und auffällig.

Im Dokument [Analyse- und Bereinigungsbausteine mit Best Practices](#) finden Sie dazu alle Analysen einzeln aufgelistet mit praktischen Anwendungsfällen.



Best Practice-Tipp: Die Einstufungen der einzelnen Analysen in die Kategorien können Sie in Ihrem CARO-System anpassen unter CARO-Konfigurationsmanager/Globale Einstellungen/Analyse/Risiko-Kategorien. Siehe auch Kapitel [Anpassung der Risikoeinstufungen](#).

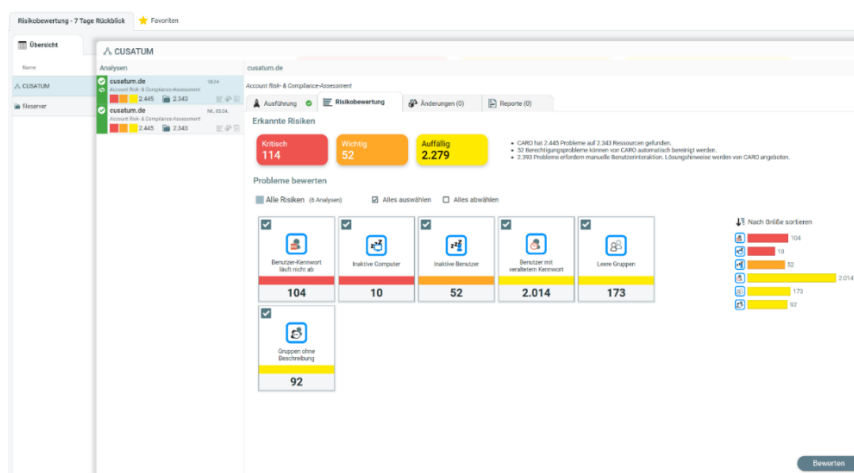
Auswahl der Systeme

Nach Klick auf das Widget Risikobewertung im Dashboard öffnet sich die Detailansicht mit einer Tabelle. Für jedes gescannte System sehen Sie Anzahl der gefundenen Probleme, jeweils einsortiert in die Risikogruppen kritisch, wichtig und auffällig:

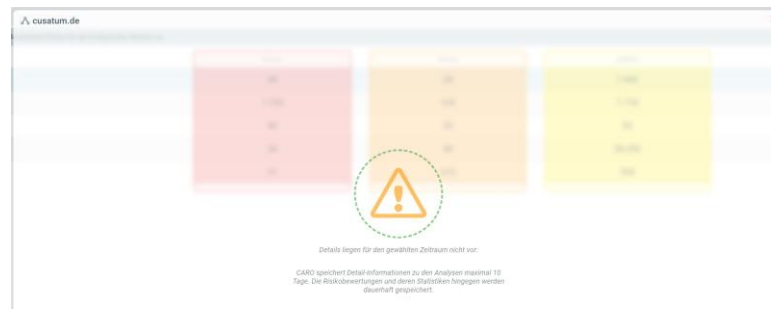
	Kritisch	Wichtig	Auffällig
CUSATUM	228	104	4.558
fileserv	6	1	0

Die gefundenen Berechtigungsprobleme werden zusätzlich über einen vorher definierten Zeitraum pro System einsortiert. Standardmäßig ist ein Rückblick auf 7 Tage konfiguriert, d.h. alle Scans der letzten 7 Tage werden für die Risikobewertung herangezogen.

Bei Selektion eines Systems in der Tabelle, z.B. die Domäne **CUSATUM** öffnet sich die Detailansicht:



Hinweis: CARO zeigt tabellarisch alle erkannten Risiken für den konfigurierten Zeitraum an. Wenn Sie einen großen Zeitraum, z.B. 30 Tage angeben, dann kann es vorkommen, dass Sie in der Detailansicht weniger oder gar keine Analysen sehen.

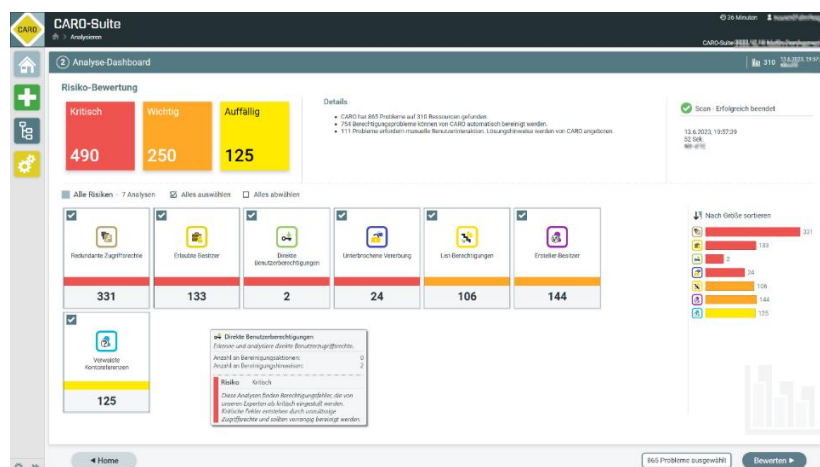
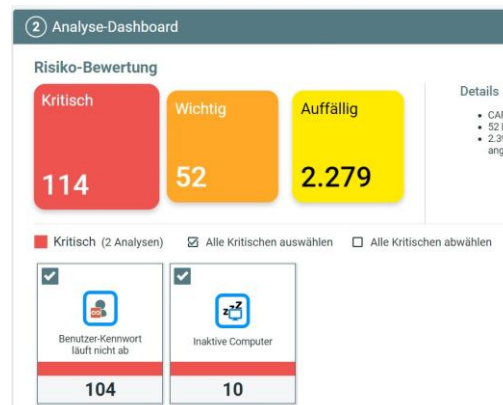


Hintergrund: CARO speichert Detail-Informationen zu den Analysen maximal 10 Tage (Standardeinstellung). Die Risikobewertungen mit den Statistiken hingegen werden dauerhaft in der Datenbank hinterlegt.

Auswahl der Berechtigungsfehler nach Analysen sortiert

Im Analyse-Dashboard sehen Sie noch einmal zusammengefasst alle Analysen mit den gefundenen Fehlern und Auffälligkeiten. Wählen Sie hier die Probleme für eine erste Bewertung aus.

Sie können die einzelnen Risikogruppen als Filter selektieren, um z.B. nur kritische Analysen anzuzeigen. Das Zurücksetzen des Risikofilters für eine bestimmte Risikogruppe, hier **kritisch**, erfolgt durch nochmaliges Anwählen der Risikokachel („Togglern“).

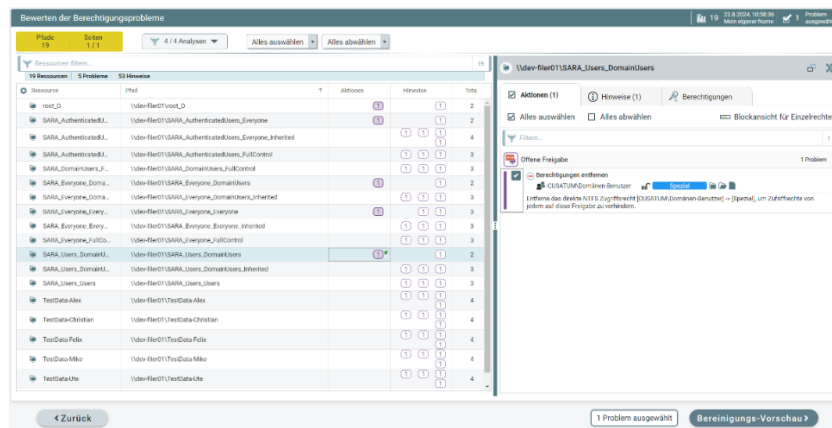




Schritt 3: Bewerten der Probleme

Nach dem Dashboard sehen Sie alle gefundenen Berechtigungsprobleme im Detail in einer tabellarischen Übersicht. Für jeden Pfad können Sie die Probleme einzeln ansehen und auswerten. Sehen Sie für jedes Problem die Zugriffsberechtigungen sowie die Vererbungslage auf der rechten Seite.

Markieren Sie die Probleme einzeln oder im Bulk zum Bereinigen.



Über den Analyse-Filter in der Leiste oben können Sie zusätzlich auf einzelne Analyse-Ergebnisse in der Ansicht filtern:



Schritt 4: Bereinigen

Alle geplanten Änderungen sind in einer kompakten Liste zusammengefasst, damit Sie abschließend Ihre Bereinigungen einfach und schnell verifizieren können. Nach Eingabe Ihres Änderungskommentars wird CARO alle Probleme bereinigen. Dies können Sie ebenfalls sofort oder zu einem späteren geplanten Zeitpunkt ausführen.



Ressource	Änderungen	Aktionen
\\freserv\testshare_prototype2	1	2
\\freserv\testshare_prototype2\Abteilungsbüro\HR\extern	1	1
\\freserv\testshare_prototype2\Abteilungsbüro\HR\extern\Anweisungen\Arbeitsanweisung\Arbeitsbereich 4	38	38
\\freserv\testshare_prototype2\Abteilungsbüro\HR\extern\Anweisungen\Offizelles Wordring	38	38
\\freserv\testshare_prototype2\Abteilungsbüro\HR\extern\Anweisungen\Sicherheitsanweisung	38	38
\\freserv\testshare_prototype2\Abteilungsbüro\IT\Linux	38	38
\\freserv\testshare_prototype2\Abteilungsbüro\IT\Linux\Standardsoftware	1	1
\\freserv\testshare_prototype2\Abteilungsbüro\IT\OS\K\Systemprogramme	38	38
\\freserv\testshare_prototype2\Abteilungsbüro\IT\Windows	1	1
\\freserv\testshare_prototype2\Abteilungsbüro\IT\Windows\Drucker\Software	38	38
\\freserv\testshare_prototype2\Automatismus\AI\Algorithmen\Geheime Projekte\VI KI	38	38
\\freserv\testshare_prototype2\Automatismus\AI\Algorithmen\Logik	38	38
\\freserv\testshare_prototype2\Automatismus\AI\Deep Learning\Versuche	38	38

2 Aktionen + - \\freserv\testshare_prototype2

- Berechtigungen hinzufügen 1 Aktion
- OS\ATUM\testshare\mars 1 Aktion
- Benutzer ändern 1 Aktion
 - Administratoren → Domänen-Administratoren
 - Benutzer von Unterordnern nicht ändern
 - Benutzer von Dateien nicht ändern

347 Probleme ausgewählt Jetzt bereinigen

Schritt 5: Dokumentieren

Nach dem Aufräumen sehen Sie in einer Übersicht den aktuellen Status Ihrer durchgeführten Bereinigung. Werden alle in diesem Scan gefundenen Probleme bereinigt, beträgt der Fortschritt 100%.



Die Anzahl der Änderungsaktionen wird ebenfalls dargestellt:



Anzeige aller Änderungen im Detail

Im Tab **Änderungen** sehen Sie alle durchgeführten Änderungen noch einmal als Liste.



Ergebnisse der Änderungen			
Zusammenfassung	Änderungen	Altknoten	Ergebnis
Report erstellen			
\\fileresult\Testshare_01\global share\projekt\17072021\17072021\report	1	1	Erfolgreich
\\fileresult\Testshare_01\global share\projekt\17072021\17072021\report	1	1	Erfolgreich
\\fileresult\Testshare_01\global share\projekt\17072021\17072021\report	1	1	Erfolgreich
\\fileresult\Testshare_01\global share\projekt\17072021\17072021\report	1	1	Erfolgreich

Hinweis: Die Anzahl der entfernten Probleme stimmt nicht immer mit der Anzahl der Änderungsaktionen überein. Die Änderungsaktionen werden vom CARO-System berechnet und werden aus Performance-Gründen zusammengefasst als Bulk-Änderungen.

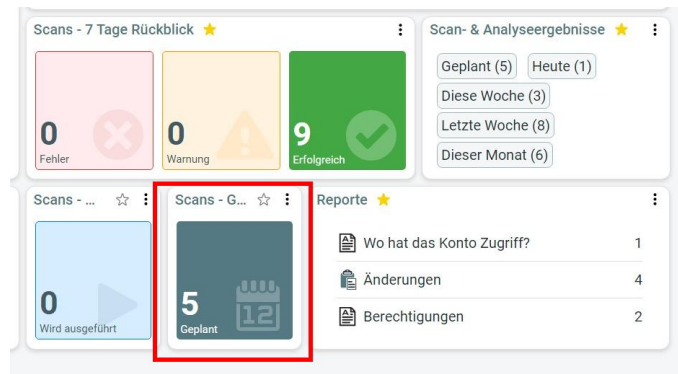
Hinweis: Haben Sie bei einer automatischen Bereinigung den Modus **Speicherbedarf minimieren** ausgewählt, werden in der Ergebnis-Liste keine Details zu den Änderungen angezeigt. Ein Report wird dann nur die Zusammenfassung ausgeben.

Sie können einen Report über alle durchgeführten Änderungen erstellen. Die Änderungen sind in der CARO-Datenbank revisionssicher protokolliert und können zu einem späteren Zeitpunkt wieder als Report aus dem System gezogen werden.

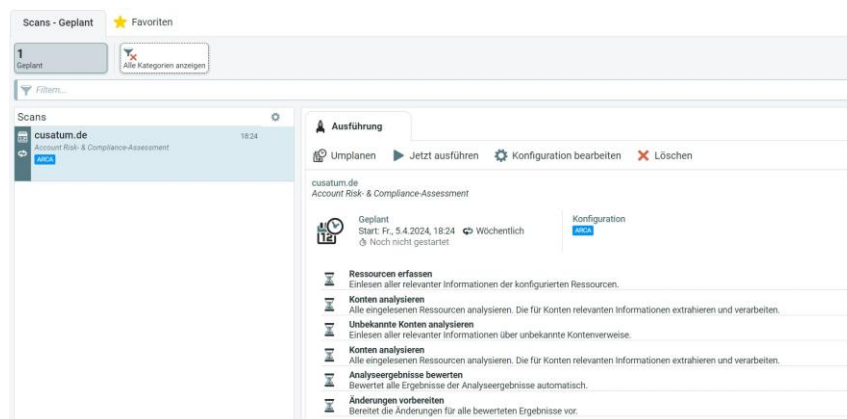
CARO Report - Modifications		Seite 1/6
Report über durchgeführte Änderungen		
Titel	Neuer Änderungsreport	
Autor	AzureAD\	
Datum	19.05.2021 10:00:19	
Kommentar	Mach weg	
Pfad-Aktionen ausgeführt	36	
\\localhost\drive\global share\Vertrieb\öffentlicher ag		
Zugriffsberechtigungen ändern		✓
Berechtigungen entfernt		
S-1-15-2-839405694-4213821001-824832031-81988	FC PD RK R W L SP M- L-	
S-1-15-2-533895992-4294967295-106324474-84779	FC PD RK R W L SP M- L-	
S-1-15-2-858889112-1178482836-135524877-80536	FC PD RK R W L SP M- L-	
S-1-15-2-248788015-4294967295-347128534-52088	FC PD RK R W L SP M- L-	
\\localhost\drive\global share\Vertrieb\Projekte		
Zugriffsberechtigungen ändern		✓
Berechtigungen entfernt		
S-1-15-2-129625072-2532751587-340180688-19271	FC PD RK R W L SP M- L-	
S-1-15-2-798882704-2015494711-444926442-46022	FC PD RK R W L SP M- L-	
S-1-15-2-494284898-4294967295-580099475-43922	FC PD RK R W L SP M- L-	
S-1-15-2-807997327-1729051578-178807251-53884	FC PD RK R W L SP M- L-	
S-1-15-2-628888144-4294967295-813076841-54295	FC PD RK R W L SP M- L-	
S-1-15-2-705927514-4294967295-877237317-58701	FC PD RK R W L SP M- L-	

Scan und Analysen wiederkehrend planen

Alle geplanten Scans und Analysen werden im Dashboard im Widget **Scans - Geplant** zusammengefasst und können von dort zentral eingesehen und nachträglich geändert werden:



Klicken Sie auf das Widget und Sie gelangen in die gefilterte Ansicht für geplante Scans:

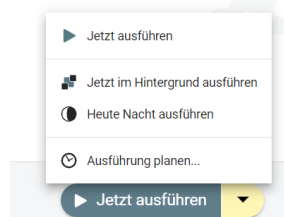


Sie können diesen Scan umplanen oder sofort neu starten. Sie können sich hier auch alle Scans anzeigen lassen, indem Sie den Filter temporär zurücksetzen:



Scans wiederkehrend planen

Vor dem Ausführen eines Scans können Sie wählen, ob Sie den Scan sofort ausführen möchten. Eine genaue Zeitplanung ist ebenfalls möglich über den Menüeintrag **Ausführung planen...**



Sie können die Scan-Wiederholungsart individuell konfigurieren, z.B. jeden Freitag in jeder Woche:



Zeitplan bearbeiten

Wählen Sie den Zeitpunkt für den Start der Aufgabe:

Erster Start: 24.2.2023 11:12

Wiederholungseinstellungen

Wiederhole:

- ☐ Nie
- ☐ Täglich
- ☒ Wöchentlich
- ☐ Monatlich
- ☐ Jährlich

Alle: 1 Woche(n)

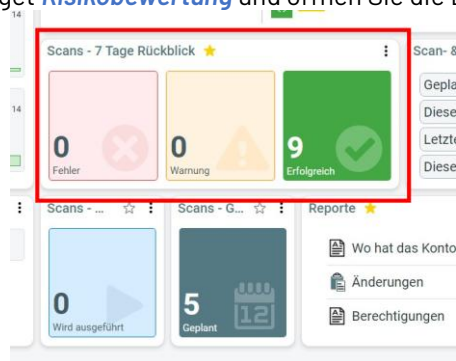
An diesen Wochentagen:

☐ Mo ☐ Di ☐ Mi ☐ Do ☒ Fr ☐ Sa ☐ So

Übernehmen Abbrechen

Auf einer bestehenden Analyse aufsetzen

Sie können Ihre begonnenen Bereinigungen einfach fortsetzen, ohne das System neu scannen zu müssen. Gehen Sie dazu im Dashboard auf das Widget **Risikobewertung** und öffnen Sie die Details-Ansicht:



Alternativ finden Sie Ihre „alte“ Scan-Übersicht im Widget **Scan- und Analyseergebnisse** wieder.

Die zuletzt ausgeführten Analysen werden in der Liste immer oben als erstes angezeigt. Eine Suchfunktion zum schnellen Auffinden Ihrer bestehenden Analysen, Änderungen oder Reporte hilft Ihnen zusätzlich.

Für jede Analyse werden in der Liste auf der linken Seite folgende Vorschau-Informationen angezeigt:

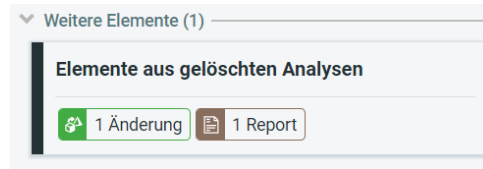
- Startzeit
- Laufzeit
- Name (Einstiegspunkte-Scan-URLs)
- Status des Scans
- Risikobewertung des Scans
- Anzahl bereits angefangener Bewertungen, falls vorhanden
- Anzahl der durchgeführten Änderungen basierend auf dieser Analyse, falls vorhanden
- Anzahl der gescannten Pfade
- Anzahl der Reporte, falls vorhanden





Was sind „Elemente aus gelöschten Analysen“?

Alle Reporte und Änderungen, bei denen die ursprüngliche Analyse gelöscht wurden, werden in diesem Sammler aufgelistet, bis sie endgültig durch den Benutzer gelöscht werden. Eine Zuordnung über eine vorher ausgeführte Analyse ist nicht mehr vorhanden, da die zugehörigen Analysen vorher gelöscht wurden und somit aus der Datenbank entfernt wurden.

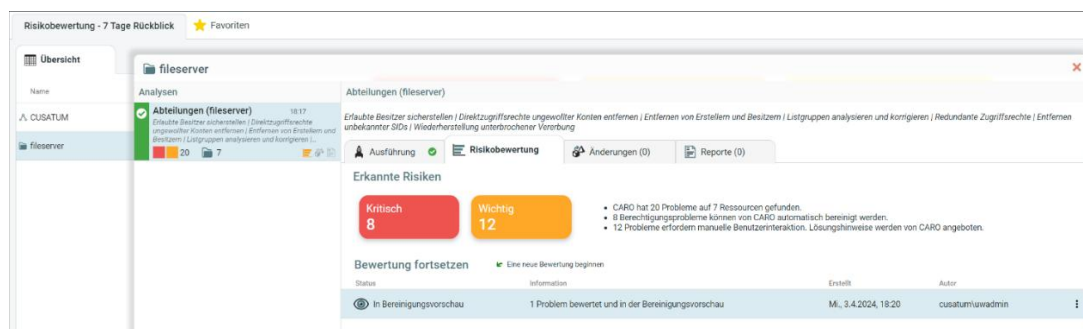


Weiter Aufräumen nach einer durchgeführten Analyse

Sie können weitere Berechtigungsfehler bereinigen durch „Letzte Bewertung fortsetzen“, indem Sie auf einer bereits durchgeführten Analyse wieder aufsetzen. Gehen Sie dazu über das Risikobewertungs-Widget auf das Tab [Risikobewertung](#).

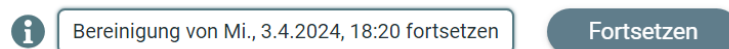


Sie können Ihre Bewertung fortsetzen, eine neue Bewertung starten, vorherigen Änderungen ansehen oder einen Report über durchgeführte Änderungen erstellen, welche CARO durchgeführt hat.



Nach einigen Bereinigungen weiter aufräumen

Falls Sie noch nicht alle Probleme in einem Schritt bereinigt haben, können Sie die restlichen Probleme auch zu einem späteren Zeitpunkt bereinigen. Dazu einfach Ihre letzte Berechtigungsänderung auswählen und [Fortsetzen](#) klicken. Sie werden direkt zur Bewerten-Ansicht geleitet und können hier weitere Probleme zum Bereinigen auswählen:



Reporte anzeigen oder herunterladen

Zu jeder durchgeführten Änderung kann ein Report erstellt werden. Die Daten dazu sind in der CARO-Datenbank hinterlegt. Alle bereits erstellten Reporte werden bei der Analyse aufgelistet und können dann zu einem beliebigen Zeitpunkt vom Server heruntergeladen oder angezeigt werden. Reporte sind derzeit im PDF-Format verfügbar. Wenn Sie im Browser ein PDF-Plugin installiert haben, können Sie sich den Report sofort im Browser anschauen, da ein neues Tab-Browser-Fenster geöffnet wird.

Alle Reporte sind über das Report-Widget einsehbar. Die CARO-Suite sortiert die verschiedenen Report-Typen in die Tab-Ansichten ein:

- Berechtigungs-Reporte: Wer hat wo Zugriff?,
- Berechtigungs-Differenz-Reporte,



- Wo hat ein Benutzer-Zugriff?,
- Bereinigungsreporte,
- Analyse-Reporte,
- Übersichtsstatistiken zu Bereinigungen,
- Vereinfachte Zugriffsrechte.

The screenshot shows the 'Reporte' widget with a 'Favoriten' star icon. Below the header, there are tabs for 'Alle (2)' and 'Berechtigungen (2)'. A search bar labeled 'Filtern...' is present. The table below lists two reports:

Status	Status	Status	Titel	Autor	Sprache	Aktionen
✓	So., 7.4.2024, 20:05	\\fileservers\Abteilungen\IT	Neuer Berechtigungs-Report - IT	cusatum\uwadmin	Deutsch (Deutschland)	
✓	So., 7.4.2024, 20:05	\\fileservers\Abteilungen	Neuer Berechtigungs-Report - \\fileservers\Abteilungen	cusatum\uwadmin	Deutsch (Deutschland)	

Das Reporte-Widget zeigt jeweils die Anzahl der erzeugten Reporte pro Kategorie an:

The screenshot shows the 'Reporte' widget with a 'Favoriten' star icon. Below the header, there is a list of reports with their respective counts:

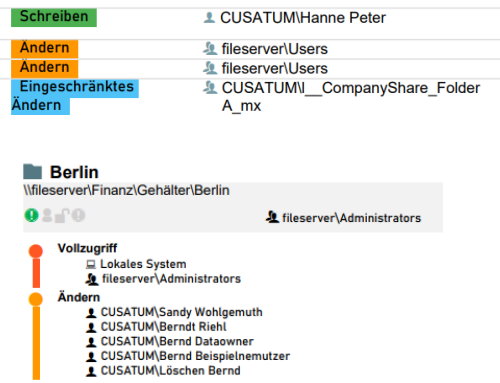
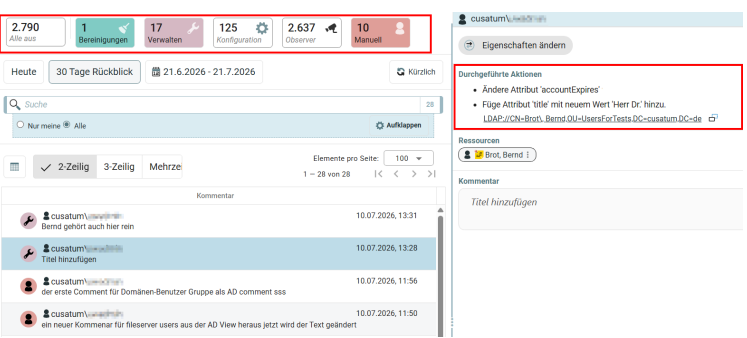
Reporte	Anzahl
Wo hat ein Benutzer/Gruppe Zugriff?	231
Analysen	45
Bereinigungen	42
Übersichts-Statistiken	66
Wer hat wo Zugriff?	87
Vereinfachte Zugriffsrechte	203



Dokumentieren

Alle Änderungen, Prozesse und Ergebnisse werden revisionssicher dokumentiert und in klaren, professionellen Reports aufbereitet – für maximale Nachvollziehbarkeit und eine Compliance, auf die Sie sich verlassen können.

Funktionsüberblick

Funktion	Umsetzung
Reporte • Wer hat wo Zugriff? • Wo hat ein Benutzer/Gruppe Zugriff? • Berechtigungsdifferenzen in historisch gewachsenen Strukturen • Analyse-Reporte • Bereinigungen • Statistiken • Reporte für Data Owner	 The screenshot shows a 'Schreiben' (Write) action being performed on a folder structure. It lists users like 'CUSATUM\Hanne Peter', 'fileserv\Users', and 'CUSATUM\CompanyShare_Folder A_mx'. Below, it shows a 'Berlin' folder path and a list of users with their permissions, including 'fileserv\Administrators' and 'CUSATUM\Sandy Wohlgemuth'.
Globales Logbuch – Revisionssichere Protokollierung Alle Änderungen werden zentral dokumentiert und sind jederzeit nachvollziehbar. Filter nach Zeitraum, Autor, Konto- oder Verzeichnis-Namen sowie einer bestimmten Ticket-ID sind möglich.	 The screenshot displays the 'Globales Logbuch' interface. It features a top bar with statistics (2.790, 1, 17, 125, 2.637, 10) and a search bar. Below, there's a list of events with columns for date, time, and user. A sidebar on the right shows 'Durchgeführte Aktionen' (Performed Actions) and 'Ressourcen' (Resources).



Logbuch an Konten, Verzeichnissen und der Konfiguration

Alle Änderungen durch die CARO-Suite werden an Konten, Verzeichnissen und an Konfigurationseinstellungen revisionssicher hinterlegt.

The screenshot shows the 'Logbuch' (Logbook) interface. At the top, there's a header for 'Utes neuer Ordner Nummer 2' with buttons for 'Neuer Eintrag', 'Export Excel', and 'Aktualisieren'. Below this is a filter section with 'Nur meine' and 'Alle' options. A table lists log entries with columns for 'Typ', 'Erstellt', and 'Autor'. The entries show dates like 16.02.2026, 09.02.2026, and 16.01.2026, all by 'cusatum\uwadmin'. Below the table, a detailed view of a 'Berechtigung ändern' (Change permission) entry is shown, dated 16.02.2026, 11:04. It lists changes such as creating a permission group, creating a membership, and creating a new permission group. At the bottom, there's a notification for 'Nasenbär' with 4 logbook entries, the newest being from 1.8.2025 at 11:32 by 'cusatum\...' regarding a planned change of owner.

Anpassbare Word-Templates

Basis-Reporte im PDF-Format, durch Word-Office-Vorlagen einfach an eigene Corporate-Identity anpassbar.

The screenshot shows a CARO report titled 'CARO Report – Analyse-Ergebnisse' on page 1/2. The report header includes the CARO logo and the title. Below the header, there's a section 'Report über Analyse-Ergebnisse' with fields for 'Titel' (Analyse-Report - Abteilungen (fileserv)), 'Autor' (cusatum\uwadmin), and 'Datum' (07.01.2026 17:47:12). The main content is titled 'Analyse-Übersicht' and shows a table with one entry: '5 Austausch von Berechtigungen'. To the right of the table, there's a description: 'Analyse der Berechtigung um diese gegen ein gewünschtes Zugriffsrecht auszutauschen um eine Vereinheitlichung uns sauberes Berechtigungsmanagement zu erzielen'.

Globale Einstellungen für Reporte

Datenaufbewahrung

Im CARO-Konfigurationsmanager können Sie die Richtlinien zur Datenaufbewahrung festlegen unter [Globale Einstellungen/Datenbank/Richtlinien zur Datenaufbewahrung/Reporte](#).



Global > Datenbank > Richtlinien zur Datenaufbewahrung

Reporte

Richtlinie aktiviert

☒ Wenn diese Richtlinie aktiviert ist, werden Reporte, die älter als die konfigurierten Tage sind, während der Datenbankwartung gelöscht.

Ausführung während des Hochfahrens

☐ Diese Richtlinie wird während des Startvorgangs angewendet.

Stunde der lokalen Uhrzeit

Stunde der lokalen Uhrzeit, an der diese Richtlinie angewendet wird.

1

0 - 23

Maximale Ausführungsminuten

Die maximale Ausführungszeit in Minuten. Die Ausführung wird auf unverarbeitete Daten zur nächsten geplanten Zeit fortgesetzt.

1

0 - 120

Aufbewahrungstage

Maximale Anzahl an Tagen, die Reporte gespeichert werden.

6653

2 - 7306

Ausschluss-Listen für das Auflösen von Gruppenmitgliedschaften in Reporten

Ebenfalls können Sie weitere globale Einstellungen für Reporte definieren unter [Globale Einstellungen/Reporte/Allgemein](#), u.a.

Global > Reporte

Allgemein

Maximale Anzahl der Objekte die nach Änderungen im Report ausgegeben werden sollen:

Anzahl der Objekte die nach einer Änderung im Report ausgegeben werden sollen. Die Zahl wird aus Performance-Gründen auf maximal 5.000 beschränkt.

100

1 - 5000

Maximale Anzahl der Objekte die nach einer Analyse im Report ausgegeben werden sollen:

Anzahl der Objekte die nach einer Analyse im Report ausgegeben werden sollen. Die Zahl wird aus Performance-Gründen auf maximal 5.000 beschränkt.

500

1 - 5000

Für folgende Accounts werden die Gruppenmitgliedschaft nicht aufgelöst:

Bei diesen Konten wird nur der Name aufgelöst, es werden jedoch KEINE Gruppenmitglieder angezeigt.

CUSATUM\Domain Admins				
CUSATUM\Domain Users				
CUSATUM\Testusers				
CUSATUM\Users				



Hinweis: Alle Reporte können im Design an Ihre CI (Corporate Identity) angepasst werden, da sie auf Word-Templates basieren. Für Ihre Anpassungen kontaktieren Sie bitte unseren technischen Support unter support@cusatum.de



Automatisieren

Die CARO-Suite lassen sich zentrale Mitarbeiterprozesse automatisieren.

Die Risikoanalysen liefern umfassende Handlungsempfehlungen für eine effiziente Bereinigung. Mit Smart-Permissions© lassen sich Berechtigungsgruppen automatisch erstellen. Zusätzlich können Scans bequem in der Kalenderansicht geplant und vollständig automatisiert ausgeführt werden.

Funktionsübersicht

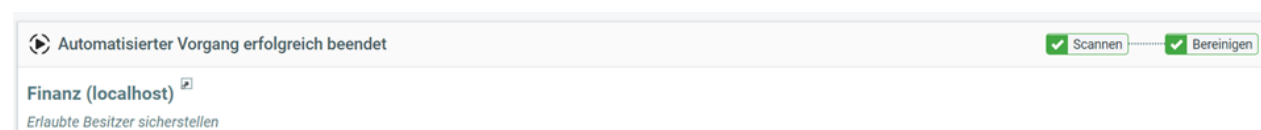
Funktion	Umsetzung
Anzeige des Bereinigungsfortschritts im CARO-Dashboard Sehen Sie, wie die CARO-Suite jeden Tag/Woche/Monat bereinigt.	
Automatisiertes Bereinigen nach jedem Scan als Option möglich Konfigurieren Sie Ihre automatische Bereinigung.	
Smart-Permissions© Automatisiertes Berechtigungsmanagement durch automatisches Erstellen von Berechtigungsgruppen.	



Benutzervorlagen – Benutzer- und Gruppen-Templates Unterstützung für standardisierte Mitarbeiterprozesse durch Benutzer- und Gruppen-Templates.	
Rest-API Umfangreiche Rest-API für die Anbindung von Mitarbeiterprozessen.	
Planbarkeit Von Scans, Analysen, Änderungen und Reporten.	

Automatisches Bereinigen mit der CARO-Suite

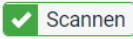
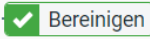
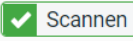
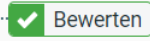
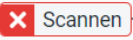
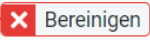
Der automatische Modus sorgt dafür, dass CARO automatisch bereinigt durchführt, wenn Berechtigungsfehler bei der Analyse gefunden wurden. Dadurch werden Ihre Prozesse automatisiert und eine manuelle Bewertung nach der Analyse ist nicht mehr notwendig.



Fortschritts-Anzeige

	System scannt noch, Bereinigen ist noch ausstehend.
	Scannen mit Analyse abgeschlossen, Bereinigen wird gerade durchgeführt.



 	Scannen und Bereinigen konnten erfolgreich ausgeführt werden.
 	Scannen mit Analyse abgeschlossen. Bewertung abgeschlossen (eine Bereinigung muss manuell erfolgen).
 	Scannen und Bereinigen waren nicht erfolgreich.

Konfiguration

Fast alle Bereinigungsbausteine bieten die Möglichkeit einer automatischen Bereinigung. Über Bewertungsregeln legen Sie fest, wie viele Probleme durch CARO automatisiert bewertet und anschließend bereinigt werden sollen.

Hinweis:



Falls Sie hier andere Bewertungsregeln benötigen bzw. eigene angepasste Bewertungsregeln benutzen möchten, dann wenden Sie sich bitte an unseren Support support@cusatum.de.

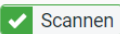
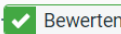
Wenn Sie alle Bewertungsregeln anwählen, wird immer die „höchste Regel“ gewinnen, d.h. **Bereinige alles** ist höher bewertet als **Bereinige 20.000**.

Bei Bewertungsvorschau anhalten (nur Bewerten)

In der Konfiguration können Sie festlegen, ob Sie im automatischen Modus nur bis zum Schritt Bewerten gehen wollen. Dazu wählen Sie bitte die Auswahlbox: „Bei 'Bewertungsvorschau' anhalten zum Prüfen“ an:

☒ Bei 'Bewertungsvorschau' anhalten zum Prüfen

Der Bereinigungsprozess wird mit der Vorschau gestoppt. Sie können alle nach der Bewertungsregel gefundenen Probleme noch einmal überprüfen. Die Änderungen werden in einer Bewertungsliste abgespeichert und können später manuell bereinigt werden.

Diese Option ist z.B. dann sinnvoll, wenn Sie noch einmal manuell überprüfen wollen, welche Fehler CARO gefunden hat. Das System speichert die Bewertung ab und alle gefundenen Fehler können Sie nachträglich in der Bewerten-Ansicht einsehen und kontrollieren.

Schritte zum Navigieren in die Bewertungsvorschau

Gehen Sie dazu auf die Risikobewertung im Dashboard, selektieren Sie Ihr System und Ihren Scan und navigieren Sie abschließend über „Fortsetzen“ zur Ansicht für alle gefundenen Fehler und den daraus resultierenden Bereinigungen bzw. Änderungen.



1. Risikobewertung-Widget selektieren



2. System auswählen

Wählen Sie in der Liste Ihrer gescannten Systeme das System aus, für welches Sie eine Bewertung fortsetzen wollen.

Risikobewertung - 7 Tage Rückblick			
★ Favoriten			
Übersicht			
Name	Kritisch	Wichtig	Auffällig
cusaturn	228	104	4.558
fileserver	6	1	0

3. Berichtigungsvorschau ist vorhanden

Alle vorhandenen Analysen für ein System werden in einer Liste angezeigt. Jede Analyse zeigt durch farbige Symbole an, ob eine Bewertung, eine Bereinigung oder Reporte vorhanden ist. Die Symbole stellen Platzhalter dar und sind standardmäßig grau dargestellt.

Analysen		
✓	cusaturn.de	Do., 04.04.
	Account Risk- & Compliance-Assessment	
	2.445	2.343
✓	cusaturn.de	Mi., 03.04.
	Account Risk- & Compliance-Assessment	
	2.445	2.343

Eine vorhandene Bewertung wird farbig markiert.



Das gleiche Prinzip gilt für eine vorhandene Änderung oder einen erstellten Report, der Platzhalter ist dann auch jeweils farbig markiert.

4. Bereinigung fortsetzen

Sie können die Bereinigung nun manuell fortsetzen, welche beim automatischen Bereinigungsvorgang angehalten wurde.

Fortsetzen

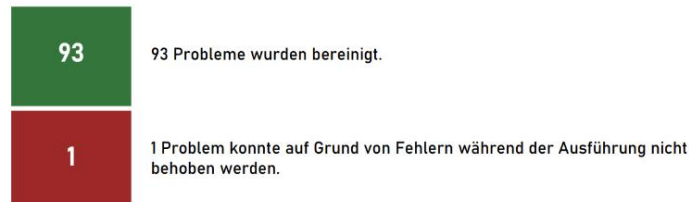
k und verbraucht dadurch



Report über durchgeführte Änderungen

Titel	Unit-Test report title
Autor	Rudy Report
Datum	27.03.2020 13:08:34
Kommentar	comment

Änderungszusammenfassung



Änderungsübersicht

Einstiegspunkt	Analyse	Ergebnis	Anzahl
C:\temp	Unresolved Account References	✓ Erfolgreich ✗ Zugriff verweigert	93 1

Änderungsdetails

C:\temp\test1	Change permissions Remove unresolved SID S-1-5-32-12345-67890-00742 with access rights 'Modify'.	✓
C:\temp\test1\failed	Change permissions Remove unresolved SID S-1-5-32-12345-67890-00742 with access rights 'Modify'.	✗ Zugriff verweigert
C:\temp\test2	Change permissions Remove unresolved SID S-1-5-32-12345-67890-00743 with access rights 'Read & Execute'.	✓



Hinweis: Wenn mehr als **100** Berechtigungsfehler gefunden und automatisch bereinigt wurden, wird der Report nur eine Zusammenfassung der Fehler anzeigen. Die Änderungsdetails als Liste werden nicht mit im Report aufgelistet.

Ressourcen-Ansicht zur Berechtigungsanalyse



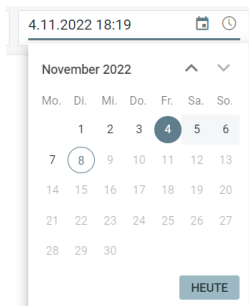
Öffnen Sie die Ressourcen-Ansicht direkt über die CARO-Menüleiste:

Die Ressourcen-Ansicht zeigt zu einem gewählten Datum für alle durchgeführten Scans die Berechtigungslage an. Derzeit werden AD-Strukturen und Fileserver-Strukturen (mit lokalen Konten) unterstützt. Sie können über eine Navigationsleiste durch die Ordner-Strukturen navigieren, Ordner suchen und sich die Berechtigungen und Zugriffsrechte anzeigen lassen.

Ressourcen filtern...						3
	Name	Scan-Zeit	Auffälligkeiten hier	Auffälligkeiten unterhalb	Besitzer	Verteilung der Berechtigungen
Filesystem						
	 \\localhost\drived	8.11.2022, 18:19		 	  Unbekannt	 
Active Directory						
	 cusatum.de	8.4.2022, 18:32		 	 Administrators	   
Lokale Konten						
	localhost	8.11.2022, 18:19				



Standardmäßig werden immer die neuesten Scans pro Technologie angezeigt. Die Auswahl eines älteren Scans erfolgt über die Kalender-Datumsauswahl. Der Kalender zeigt nur den Zeitraum zwischen dem ältesten und dem neuesten Scan-Datum an. Alle Scan-Zeiten dazwischen können Sie frei auswählen. CARO wählt automatisch die passenden Scans zu dem ausgewählten Datum aus.



Live-Anzeige der Ist-Berechtigungen

Mit der Live-Anzeige für Ist-Berechtigungen sehen Sie in **Echtzeit**, wer welche Zugriffsrechte hat, und das ganz ohne aufwendige Datenbankabfragen.

Sobald Sie die Ressource-Ansicht öffnen, sind alle Berechtigungen direkt verfügbar, ohne Verzögerung und ohne zusätzliche Infrastruktur. So behalten Sie jederzeit den kompletten Überblick und sparen wertvolle Zeit bei der Berechtigungsprüfung.

- Sofortige Sichtbarkeit aller Berechtigungsänderungen
- Übersichtliche Darstellung komplexer Zugriffsrechte auf einen Blick
- Weniger "Blindflug" bei der Verwaltung kritischer Zugriffsrechte

Name	Aufzählungen	Besitzer	Verteilung der Berechtigungen
Active Directory			
cusatum			
Filesystem			
Abteilungen		CUSATUM\wladimir	
dev-...		CUSATUM\wladimir	
Finanz		CUSATUM\wladimir	
GF		fileserv\Administrators	
IT		fileserv\Administrators	
Marketing		CUSATUM\wladimir	
Personal		CUSATUM\wladimir	
Lokale Konten			
dev-...			
Microsoft Entra ID			
cusatum.de			

Konto	Berechtigung	Anwenden auf
Lokales System	Vollzugriff	
fileserv\Administrators	Vollzugriff	11
CUSATUM\wladimir	Vollzugriff	
CUSATUM\Group 0	Ändern	12
CUSATUM\wladimir	Lesen & Ausführen	
CUSATUM\Group 0	Lesen & Ausführen	12
CUSATUM\wladimir	Spezial	

Konto	LDAP-Container	Direkt	Indirekt	Ebene
CUSATUM\Ampel, Anna	CARO			2
CUSATUM\wladimir	Users			2
CUSATUM\Felix Frieß	UsersForFests			2
CUSATUM\Lore All	Users			2

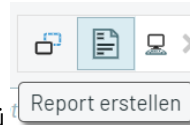
Direktes Berechtigungsmanagement

Keine umständlichen Prozesse und komplizierten Befehlszeilen mehr: Mit dem neuen CARO-Management greifen Sie direkt in Ihre Berechtigungsstrukturen ein. Eine einfache **Anbindung von eigenen Skripten** für das direkte Managen ist ebenfalls möglich.



Berechtigungsreporte erstellen

In dieser Ansicht können Sie ebenfalls Berechtigungsreporte erstellen: einen Report über die IST-Berechtigungslage, einen vereinfachten Zugriffsrechte-Report für Data Owner, einen Differenz-Report über geänderte Berechtigungen unterhalb oder den Use-Case-Report: Wo hat ein Benutzer/Gruppe Zugriff.

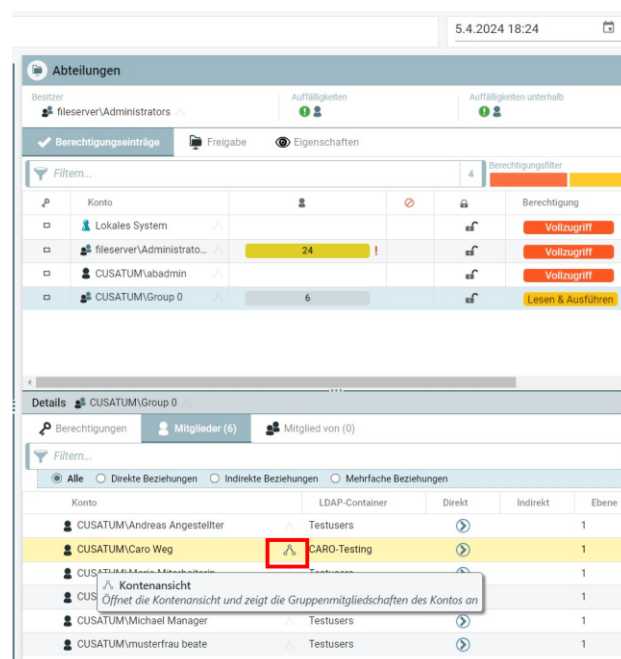


In der Navigationsleiste wird dazu das Reporte-Kontext-Menü angeboten:



Von einem Konto in die Kontenansicht navigieren

Für jedes angezeigte Konto in der Ressourcenansicht können Sie in die neue Kontenansicht wechseln, um sich mehr Details zu einer Gruppe oder einem Benutzer-Konto anzeigen zu lassen. Selektieren Sie dazu den Account, um die Schaltfläche  zu aktivieren.



Die Benutzung der Kontenansicht mit Suchfunktion wird im Kapitel [Account-Ansicht mit Suchfunktion](#) näher erläutert.

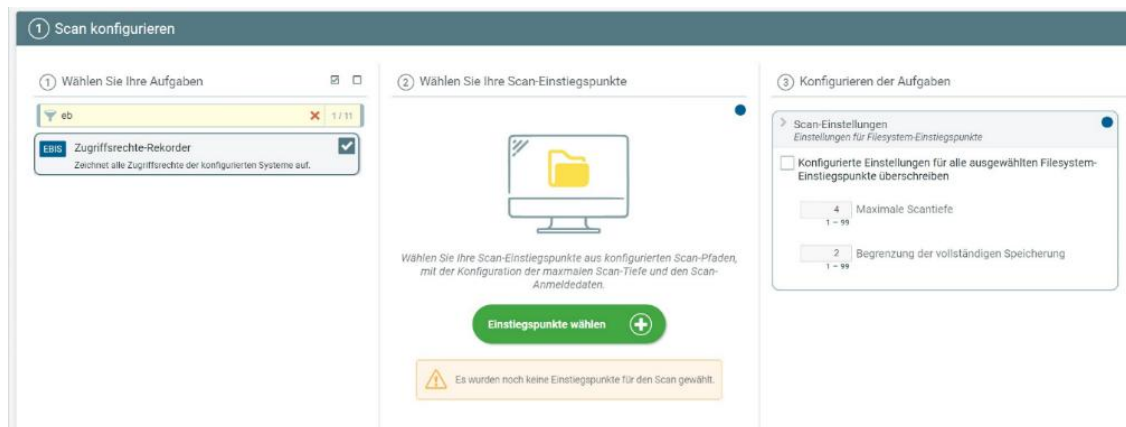
Eine IST-Berechtigungsanalyse starten

EBIS

Für die Anzeige Ihrer IST-Berechtigungslage ist nur der Baustein  notwendig. Zum Scannen der Berechtigungen gehen Sie links im CARO-Menü zu „Neue Analyse starten“.



Wählen Sie nur den Baustein EBIS aus. Nach Auswahl Ihrer gewünschten Scan-Einstiegspunkte starten Sie den Scan mit der integrierten Analyse der Berechtigungen bzw. Konten.



Der Baustein EBIS ist selektiert:

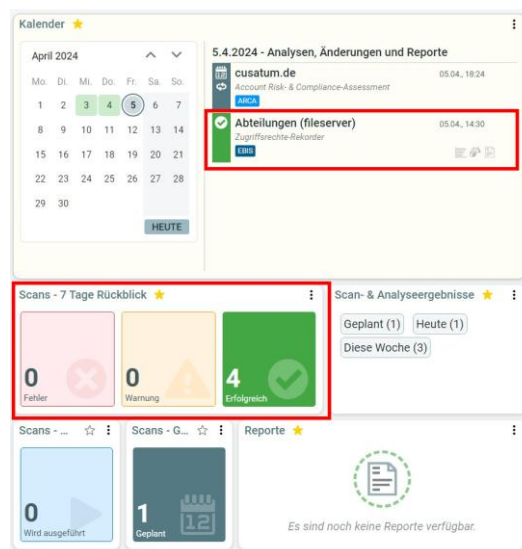
Auf der rechten Seite unter „3. Konfigurieren der Aufgabe“

werden alle für den Start von EBIS notwendigen Parameter angezeigt



Hinweis: Auch für bereits durchgeführte Scans mit anderen Bausteinen, wie z.B. ERBE, TEUS oder BAKS werden Zugriffsrechte in der Ressourcen-Ansicht angezeigt. Diese Bausteine erfassen ebenfalls die Berechtigungen, mit Ihnen können zusätzlich noch Bereinigungen mit CARO durchgeführt werden.

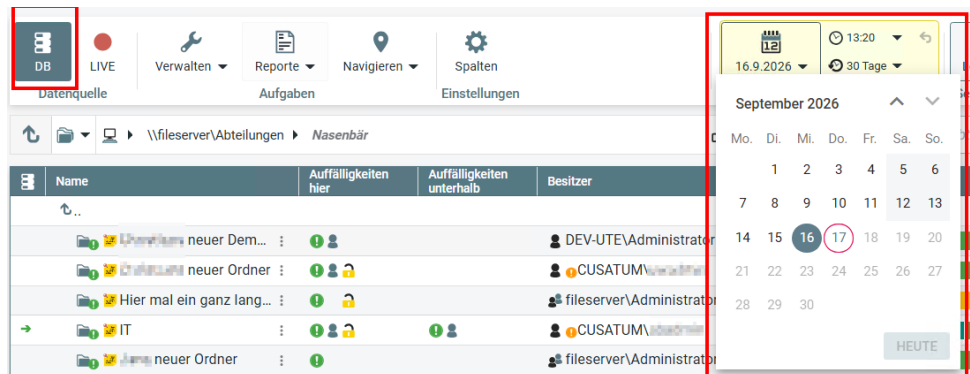
Ein erfolgreicher Scan mit EBIS ist dann im Dashboard im Widget **Scans** oder **Kalender** zu finden:



Öffnen Sie über das CARO-Menü direkt die Ressourcenansicht, um die IST-Berechtigungssituation anzuzeigen. Die Daten vom Scan sind in der CARO-Datenbank hinterlegt und können über die Toolbar ausgewählt werden.



Wählen Sie dazu als Datenquelle DB aus und suchen sich Ihre Scan Zeit. Standardmäßig wird neueste Scanzeit aus der Datenbank benutzt.



Anzeige von Berechtigungs-Anomalien

In der Ressourcen-Ansicht sehen Sie veränderte Berechtigungen und veränderte Besitzer unterhalb auf einem Blick. Ebenfalls werden unterbrochene Vererbungen, nicht kanonische ACL-Strukturen oder leere ACLs erkannt und angezeigt.

Auffälligkeiten hier	Auffälligkeiten unterhalb	Besitzer
		Unbekannt
		Administratoren
...		
		Administratoren
		Administratoren
		Administratoren
		Administrator
		Administrator
		Administratoren
		Administratoren
		Administrator
		Administratoren
		Administratoren
		Administratoren
		Administratoren
		Administratoren
		Administratoren

Verteilung von Berechtigungen (Statistiken)

Die Verteilung der Berechtigungskategorien sehen Sie jeweils rechts als farbiges Balkendiagramm pro Verzeichnis. So haben Sie einen schnellen Überblick über Abweichungen in Ihrer Berechtigungsvergabe. Vergleichen Sie direkt die Ordnerberechtigungen einer Verzeichnisebene miteinander auf der linken Seite oder sehen sich pro Verzeichnis die Details auf der rechten Seite an.

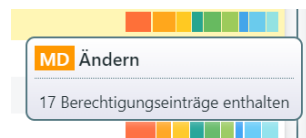


Ressourcen unterhalb von 'global share' filtern...

Name	Scan-Zeit	Auffälligkeiten hier	Auffälligkeiten unterhalb	Besitzer	Verteilung der Berechtigungen
Vocalhost\drived	8.11.2022, 18:19	0	0	Unbekannt	
global share	8.11.2022, 18:19	0	0	Administratoren	
Kinder von global share					
Archive	8.11.2022, 18:19	0	0	Administratoren	
Backup	8.11.2022, 18:19	0	0	Administratoren	
Finanz	8.11.2022, 18:19	0	0	Administratoren	
Friedhof	8.11.2022, 18:19	0	0	Administrator	
GF	8.11.2022, 18:19	0	0	Administrator	
Home	8.11.2022, 18:19	0	0	Administratoren	
IT	8.11.2022, 18:19	0	0	Administratoren	
Illegal	8.11.2022, 18:19	0	0	Administrator	
Marketing	8.11.2022, 18:19	0	0	Administratoren	
Personal	8.11.2022, 18:19	0	0	Administratoren	
This is a very long ...	8.11.2022, 18:19	0	0	Administratoren	
Vertrieb	8.11.2022, 18:19	0	0	Administratoren	
global share	8.11.2022, 18:19	0	0	Administratoren	

Elemente pro Seite: 100 1 – 13 von 13 |< >| Gehe zu Seite: 1

Über einen Tooltip bei Mouse-Hover sehen Sie zusätzlich die Anzahl der Berechtigungseinträge pro Berechtigungskategorie:



Anzeige von Scan-Fehlern und Scan-Warnungen

Aufgetretene Fehler oder Warnungen vom Ressource-Scan werden direkt an der Ressource als kleiner Kreis dargestellt, bei Fehlern in Rot, bei Warnungen in Orange.

Folder	15.6.2022, 10:35
NFS-Testshare	10.2.2023, 15:07
NewShare	10.2.2023, 15:07

In den Details rechts werden alle Fehler und Warnungen aufgelistet:

Folder

Besitzer

Administrator

Auffälligkeiten

!

✓ Berechtigungseinträge

⚠ Scan-Probleme (1)

Warnungen (1)

⚠ Ignoriert - maximale Scantiefe überschritten.

Informationen zu einzelnen Berechtigungseinträgen werden rechts auf der Seite angezeigt:



Details: CUSATUM/Exchange Servers

Konto	LDAP-Container	Direkt	Indirekt	Ebene
Exchange Install Domain Servers	Microsoft Exchange System Objects	>		1
EXCHANGE	Servers	>	(1x)	2

Ressourcenansicht: Berechtigungsdetails für Bob Baumeister

Anzeige von gelöschten Konten mit Konteninformation

CARO zeigt nun auch an, wann Konten beim Scannen als gelöscht erkannt wurden, mit Datumsanzeige im Tooltip. Sie erkennen solche Konten an einem kleinen roten Kreuz . Der Name des Kontos wird weiterhin angezeigt, da CARO in einem vorherigen Scan diese Kontoinformation gespeichert hat.

Berechtigungseinträge

Konto	Berechtigungen
Administratoren	1
Mary Dole	
Nereo Ferrau	
S-1-5-21-1332380298-428...	
Jeder	

Tooltip for Mary Dole:
 ID S-1-5-21-1332380298-4281389868-1580002489-1227
 Als gelöscht erkannt am 10.11.2022, 13:37:43

Anzeige der Berechtigungskategorien

Standardmäßig werden alle Berechtigungskategorien auf der rechten Seite im Seitenpanel unter Berechtigungen angezeigt:



Konto	Berechtigung	Anwenden auf
Lokales System	Vollzugriff	[Icons]
fileservers\Administrators	Vollzugriff	[Icons]
CUSATUM\...	Vollzugriff	[Icons]
CUSATUM\Karlpete Lucas	Ändern	[Icons]
CUSATUM\Hanne Peter	Ändern	[Icons]
CUSATUM\Abteilungen_...	Ändern	[Icons]
CUSATUM\Group 0	Ändern	[Icons]
CUSATUM\...	Ändern	[Icons]
CUSATUM\Abteilungen_...	Lesen & Ausführen	[Icons]
CUSATUM\...	Lesen	[Icons]
CUSATUM\Peter One	Schreiben	[Icons]
CUSATUM\Peter 42	Schreiben	[Icons]
CUSATUM\Hanne Peter	Schreiben	[Icons]
CUSATUM\Peter Parker	Schreiben	[Icons]
CUSATUM\Meter, Peter	Schreiben	[Icons]
CUSATUM\Group 0	Spezial	[Icons]

Sie können Ihre angezeigten Kategorien einschränken in der Globalen Konfiguration im Konfigurationsmanager:

Berechtigungen

Angezeigte Berechtigungskategorien

Die Liste der anzuzeigenden Zugriffsrechtskategorien. Bei einer leeren Liste werden alle Kategorien angezeigt. Nicht selektierte Kategorien werden ausgeblendet.

Vollzugriff, Ändern, Lesen, Schreiben

Bearbeitbare Berechtigungskategorien

Die Liste der Bearbeitbaren Zugriffsrechtskategorien. Bei einer leeren Liste sind alle Kategorien Bearbeitbar. Nicht ausgewählte Kategorien sind schreibgeschützt oder ausgeblendet.

Ändern, Lesen & Ausführen, Schreiben, Spezial

Nach Speichern der Änderungen sehen Sie in der Ressourcenansicht nur noch alle Berechtigungen für die Gruppen, Vollzugriff, Ändern, Lesen und Schreiben:



neuer Ordner Nummer 3

Berechtigungen Aufgaben Logbuch Attribute

neuer Ordner Nummer 3
\\fileserv\Abteilungen\neuer Ordner Nummer 3

Besitzer: fileserv\Administrators 7 Logbucheinträge Scan-Zeit: 19.9.2026, 10:12:38 Vererbung:

Verwalten Berechtigungen Reporte

Berechtigungen

Filtern... 14 Anzeigefilter für Berechtigungen

Konto	Berechtigung	Anwenden auf
Lokales System	Vollzugriff	
fileserv\Administrators	Vollzugriff	
CUSATUM\	Vollzugriff	
CUSATUM\Karl peter Lucas	Ändern	
CUSATUM\Hanne Peter	Ändern	
CUSATUM\Abteilungen\neuer	Ändern	
CUSATUM\Group 0	Ändern	
CUSATUM\	Ändern	
CUSATUM\	Lesen	
CUSATUM\Peter One	Schreiben	
CUSATUM\Peter 42	Schreiben	
CUSATUM\Hanne Peter	Schreiben	
CUSATUM\Peter Parker	Schreiben	
CUSATUM\Meter, Peter	Schreiben	

Berechtigungs-Reporte

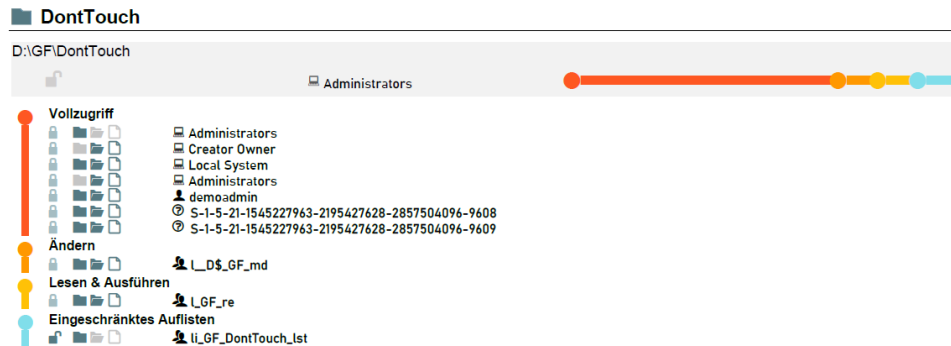
Über die Ressourcen-Ansicht können Sie für alle Verzeichnis-Ebenen Berechtigungsreporte erstellen. Alle Reporte werden im CARO-Dashboards im Widget **Reporte** gesammelt und können von dort heruntergeladen, gelöscht oder neu erstellt werden, z.B. wenn Sie den Report in einer anderen Sprache erstellen wollen.

Report über die IST-Berechtigungssituation

Für diesen Report werden folgende Standardparameter genutzt:

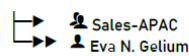
- Anzeige aller geänderten Unterverzeichnisse unterhalb des ausgewählten Verzeichnisses
- Bis zur Ebene 8
- Zeige Anomalien an
- Zeige Propagation-Flags an
- Zeige den Besitzer an
- Zeige die Zugriffsrechte-Verteilung als Farb-Balken an

Die Details für ein Verzeichnis werden im Report so ausgegeben:



Gruppen und deren Mitglieder werden am Ende der Berechtigungsliste im Report aufgelistet, dabei werden direkte und indirekte Mitglieder angezeigt:

I_Vertrieb_Hersteller_md

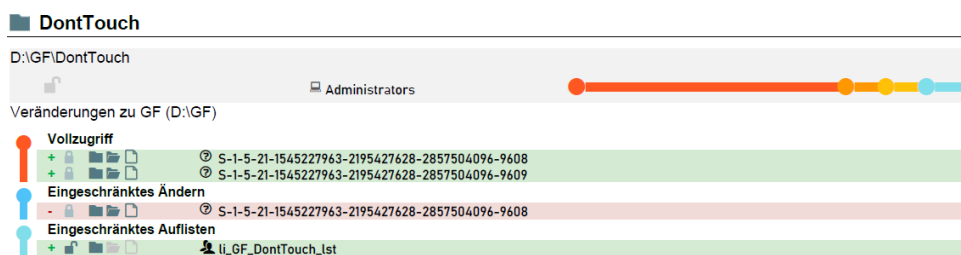


Berechtigungs-Differenz-Report

Für diesen Report werden folgende Standardparameter genutzt:

- Anzeige aller geänderten Unterverzeichnisse unterhalb des ausgewählten Verzeichnisses
- Anzeige der hinzugekommenen Berechtigungseinträge
- Anzeige der weggenommenen Berechtigungseinträge
- Bis zur Ebene 8
- Zeige Anomalien an
- Zeige Propagation-Flags an
- Zeige den Besitzer an
- Zeige die Zugriffsrechte-Verteilung für das Verzeichnis als Farb-Balken im Header an

Die Details für ein Verzeichnis werden im Report so ausgegeben:



Use-Case-Report: Wo hat ein Benutzer/Gruppe Zugriff?

Diesen Report können Sie derzeit nur direkt in der Detail-Ansicht beim selektierten Konto erstellen. In der Account-Headerleiste rechts unten finden Sie die Schaltfläche zum Starten des Reports. Ab diesem Pfad werden alle Pfade unterhalb analysiert, wo und welche Zugriffe das selektierte Konto hat:





drived		Das Verzeichnis			
Besitzer	S-1-5-21-4262257557-526714673-2123679...	Auffälligkeiten	Keine	Auffälligkeiten unterhalb	
Berechtigungsbeiträge Freigabe Eigenschaften					
Filtern...		6	Berechtigungsfilter		
Konto				Berechtigung	
S-1-5-21-4262257557-526...				Vollzugriff	
Administratoren	2			Vollzugriff	
Lokales System				Vollzugriff	
S-1-5-21-4262257557-526...				Ändern	
Authentifizierte Benutzer				Ändern	
Benutzer	2			Lesen & Ausführen	

Im Reportdialog können Sie die Sprache und einen Titel festlegen:

Reporterstellung

Report 'Wo hat das Konto Zugriff?'

Titel

Report Wo hat das Konto 'Benutzer' Zugriff?

Format

PDF-Dokument

Sprache

Deutsch (Deutschla...)

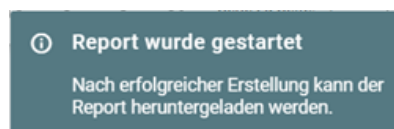
Erstellen

Schließen

Für diesen Report werden folgende Standardparameter genutzt:

- Überprüfung aller geänderten Unterverzeichnisse unterhalb des ausgewählten Verzeichnisses
- Bis zur Ebene 8
- Zeige Berechtigungszugriffe des Kontos an mit Gruppenmitgliedschaften
- Jeder-Konto ist nicht eingeschlossen in der Suche
- Authentifizierte Benutzer ist nicht eingeschlossen in der Suche
- Domänen-Benutzer ist nicht eingeschlossen in der Suche

Das Erstellen des Reports wird im Hintergrund ausgeführt, sie werden mit einem Hinweis darüber informiert:



Sie finden den fertig erstellten Report später im Dashboard im Widget **Reporte**. Alle anderen erstellten Reporte, auch Ihre Änderungsreporte von Bereinigungsverfahren, können Sie dort öffnen oder auch löschen.

Beispiel für einen Use-Case-Report:



Wo hat das Konto 'Blom, Mattias' Zugriff? Seite 2/3

Blom, Mattias

Name	URI	Zugriffsrecht	Berechtigtes Konto
Marketing	Organization/Marketing	Ändern Eingeschränktes Auflisten	Blom, Mattias li_Organization_Marketing_Ist
Archive	Organization/Marketing/Archive	Ändern	Blom, Mattias
2009	Organization/Marketing/Archive/2009	Ändern	Blom, Mattias
2010	Organization/Marketing/Archive/2010	Ändern	Blom, Mattias
2011	Organization/Marketing/Archive/2011	Ändern	Blom, Mattias
2012	Organization/Marketing/Archive/2012	Ändern	Blom, Mattias
2013	Organization/Marketing/Archive/2013	Ändern	Blom, Mattias
2014	Organization/Marketing/Archive/2014	Ändern	Blom, Mattias
2015	Organization/Marketing/Archive/2015	Ändern	Blom, Mattias
2016	Organization/Marketing/Archive/2016	Ändern	Blom, Mattias

Dateneigentümer-Report (Vereinfachter Zugriffsrechte-Report)

Dieser Report zeigt die Berechtigungsfehler auf einen Blick in einer einfachen Übersicht, die auch von Dateneigentümern mit wenig technischem Hintergrundwissen genutzt werden kann. Die Zugriffsrechte-Kategorien werden dabei tabellarisch aufbereitet. Zeilenweise werden die einzelnen Berechtigungseinträge aufgelistet.

	Vollzugriff	Ändern	Lesen & Ausführen	Eingeschränktes Auflisten
CUSATUM\LG_Abteilungen_IT_30_TestDaten-RW				
30_TestDaten		✓		
\\fileserver\Abteilungen\IT\30_TestDaten				
Berichte		✓		
\\fileserver\Abteilungen\IT\30_TestDaten\Berichte				

Für diesen Report werden folgende Standardparameter genutzt:

- Überprüfung aller geänderten Unterverzeichnisse unterhalb des ausgewählten Verzeichnisses
- Bis zur Ebene 8
- Zeige Berechtigungszugriffe mit Gruppenmitgliedschaften

Am Ende des Reports werden die Gruppenmitgliedschaften aufgelöst:

CUSATUM\LG_Abteilungen_IT-LIST

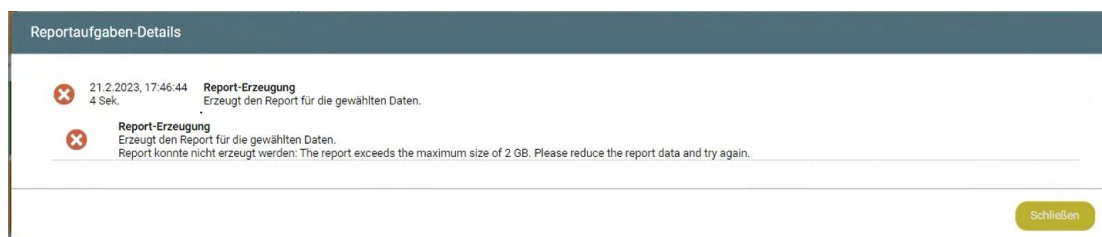
```

--> CUSATUM\Adelhard Wiechert
--> CUSATUM\Adalbert Weide
--> CUSATUM\Adelgund Mundt
--> CUSATUM\Adelgund Rahm
--> CUSATUM\Adam Bohne
--> CUSATUM\Löschen Bernd
--> CUSATUM\FG_RunScriptAfterDisable
--> CUSATUM\LG_Abteilungen_IT_30_TestDaten-RW
--> CUSATUM\LG_Abteilungen_IT_30_TestDaten_Berichte-RW
--> CUSATUM\Adalbert Rinke
--> CUSATUM\Caro.Weg
--> CUSATUM\Adelgunde Sondermann
--> CUSATUM\Adalbert Mühle

```

Erstellen von umfangreichen Reporten

Beim Erstellen von Reporten für sehr große Datenmengen kann es zu einem Abbruch der Reporterzeugung kommen. Die Report-Engine hat hier leider das Maximum von 2GB erreicht, welches das Operating-System zur Verfügung stellt.



Hinweis: Reduzieren Sie die Report-Datenmengen, z.B. bei den Berechtigungsreporten durch Auswahl von Unterverzeichnissen anstelle von ganzen Shares.

Verwalten mit der CARO-Suite

Keine umständlichen Prozesse und komplizierten Befehlszeilen mehr: Mit dem Live-CARO-Management greifen Sie direkt in Ihre Berechtigungsstrukturen ein. Eine einfache Anbindung von eigenen Skripten für das direkte Managen ist ebenfalls möglich.

Verwaltungsaufgaben mit einem Stern (*) gekennzeichnet, sind bereits als Preview-Feature verfügbar. Sie können durch unser Support-Team freigeschaltet werden, bitte wenden Sie sich dazu an [mailto: support@cusa-tum.de](mailto:support@cusa-tum.de)

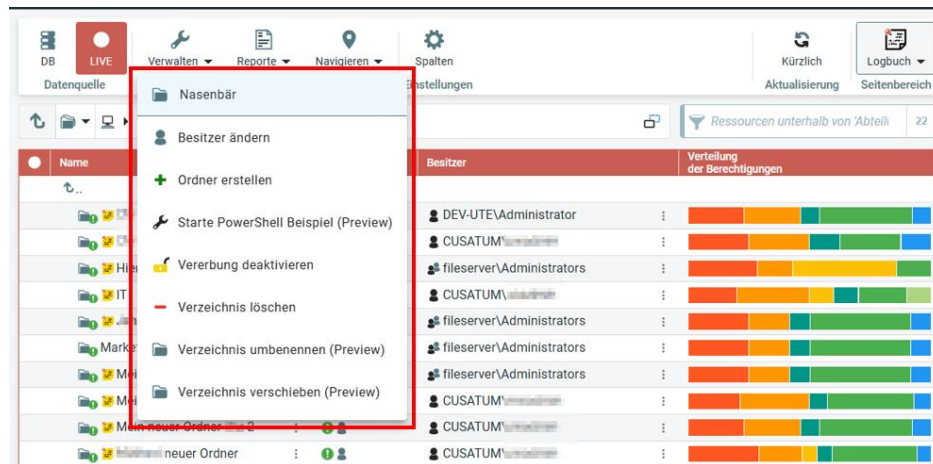
Verfügbare Technologien

Technologie	Verwaltungsaufgaben
Filesystem	10
Active Directory	13
Entra ID	5
Exchange	4

Verwaltung im Filesystem

- Verzeichnis-Vererbung ein- oder ausschalten
- Neues Verzeichnis erstellen mit oder ohne vererbte Zugriffsrechte
- Besitzer von Verzeichnissen ändern
- Verzeichnis löschen
- Verzeichnis-Zugriffsrechte entfernen
- Verzeichnis-Zugriffsrechte hinzufügen, auch mit automatisierter Gruppenerstellung dank Smart Permission©
- *Verzeichnis verschieben**
- *Verzeichnis umbenennen**

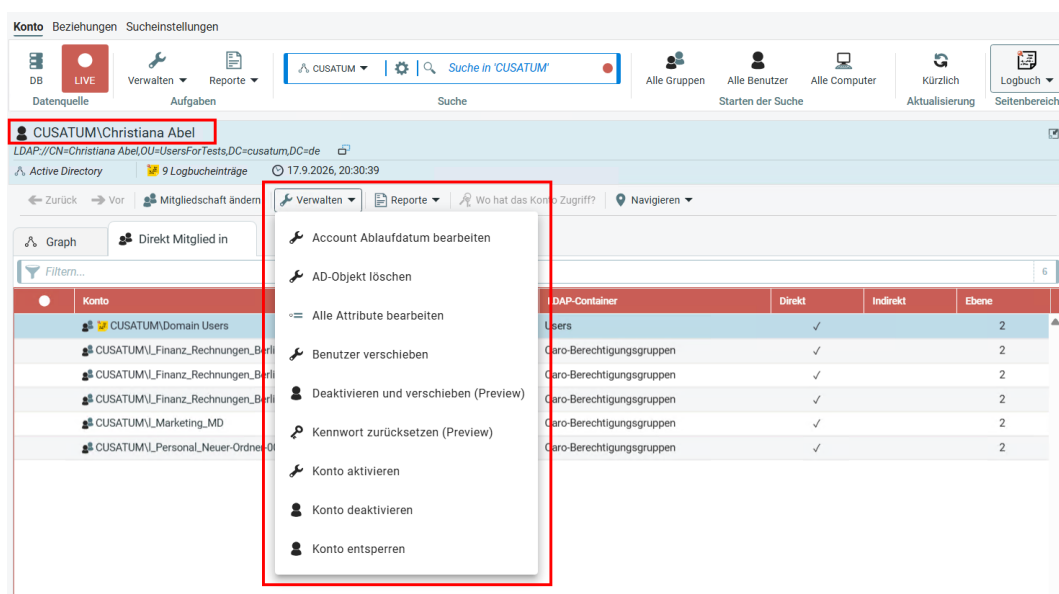
In der Ressourcenansicht finden Sie in der Toolbar unter **Verwalten** alle nutzbaren Verwaltungsaufgaben, die jeweils für das selektierte Element in der CARO-Suite zur Verfügung stehen. In diesem Beispiel werden alle Verwaltungsaufgaben für ein Filesystem-Verzeichnis im Kontextmenü angeboten:



Verwaltung im Active Directory

Verwaltungsaufgaben im Active Directory sind über die Ressourcen-Ansicht bei Unterelementen unter den Root-Ressourcen einer Domäne verfügbar. Ebenfalls in der Live-Kontenansicht, z.B. bei Gruppen oder Benutzern.

- Benutzerkonto aktivieren
- Benutzerkonto deaktivieren
- Benutzerkonto entsperren (unlock)
- AD-Objekt löschen
- Benutzer-Attribute bearbeiten
- Neue Gruppen erzeugen, direkt an der OU
- Neue Benutzer erzeugen
- Gruppenmitgliedschaften hinzufügen oder entfernen
- Benutzer verschieben
- Computer verschieben
- *Benutzerkonto deaktivieren und verschieben**
- *Benutzer-Kennwort zurücksetzen**





Verwalten im Entra ID

- One-time Passcode erstellen
- Einmaliger Zugriffspass (Temporary Access Pass, TAP) ist sinnvoll für
 - Registrierung von Methoden für Microsoft Authenticator App
 - Wiederherstellung von Authentifizierungsmethoden
 - Sicherheitsrichtlinien und Compliance: Zeitfenster für Zugriffsberechtigungen nutzen
 - Der Code wird direkt an eine ausgewählte E-Mail gesendet, z.B. den Manager des Benutzers
- Account aktivieren
 - Schnelles Reagieren von versehentlich gesperrten Benutzerkonten
- Account deaktivieren
 - Deaktivieren von Gastkonten für Zugriffsbeschränkungen
- Passwort zurücksetzen
 - Zurücksetzen eines vergessenen Passworts für ein Benutzerkonto
- Berechtigungen der CARO-Suite-App-Registrierung wiederherstellen
 - Alle erforderlichen **ReadWrite.All** Berechtigungen werden für die CARO-Suite M365 Connector App-Registrierung wiederhergestellt
 - Dies ist nur möglich, wenn die CARO-Suite M365 Connector App-Registrierung bereits folgende Berechtigung hat: **AppRoleAssignment.ReadWrite.All**

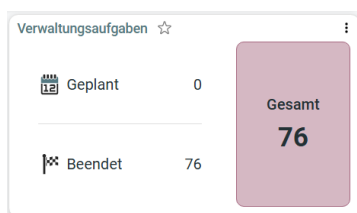
Verwalten im Exchange

- Abwesenheitsnotiz aktivieren
- Benutzerpostfach aktivieren
- Neues Benutzerpostfach erstellen
- Neues Postfach erstellen

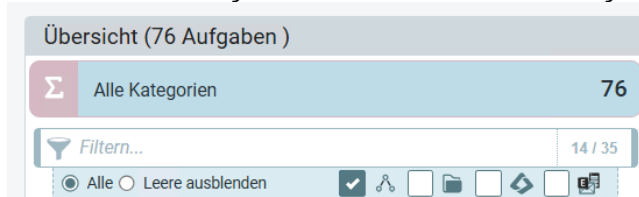
Verwaltungsaufgaben-Übersicht

Über das Widget Verwaltungsaufgaben können Sie sofort einsehen, welche Änderungen wann und von welcher Person durchgeführt wurden, bzw. über die CARO-Suite in Auftrag gegeben wurden.

Öffnen Sie dazu das CARO-Dashboard, durch Klick auf das Widget öffnet sich die Detailansicht für die Verwaltungsaufgaben.



Sie können Ihre Aufgaben filtern, z.B. nach Technologie:



Oder Sie suchen explizit nach einer Verwaltungsaufgabe, z.B. Gruppenmitgliedschaften ändern, um sich dann die Details und den zeitlichen Verlauf von allen Änderungen anzuzeigen.

Verwaltungsaufgaben
Favoriten ▾

Übersicht (76 Aufgaben)

Alle Kategorien 76

Filtern... 14 / 35

☐ Alle ☑ Leere ausblenden

Account Ablaufdatum bearbeiten Attribute bearbeiten.	0
AD-Objekt löschen Löscht ein Active Directory Objekt	0
Alle Attribute bearbeiten Alle Attribute eines Kontos bearbeiten	6
Benutzer verschieben Verschiebe das Active Directory Benutzer-Objekt zu einer anderen Organisationseinheit.	0
Computer verschieben Verschiebe das Active Directory Computer-Objekt zu einer anderen Organisationseinheit.	0
Deaktivieren und verschieben (Preview) Deaktivieren und verschieben eines Benutzers in eine OU.	0
Gruppe verschieben Verschiebe das Active Directory Gruppe-Objekt zu einer anderen Organisationseinheit.	1
Kennwort zurücksetzen (Preview) Kennwort mit einem neuen Passwort zurücksetzen.	0
Konto aktivieren Ein Benutzer- oder Computerkonto aktivieren.	0
Konto deaktivieren Ein Benutzer- oder Computerkonto deaktivieren.	1
Konto entsperren Benutzer- oder Computerkonto entsperren.	0
Kontomitgliedschaften ändern Kontobeziehungen ändern - Gruppenmitglieder oder Gruppenmitgliedschaften.	27
Neue Gruppe erzeugen Erzeugt eine neue Gruppe im Active Directory.	3
Neuen Benutzer erzeugen Erzeugt einen neuen Standardbenutzer (nativ).	2

Verwaltungsaufgaben

Filtern... 21 / 76

☐ Alle ☑ Kontomitgliedschaften ändern

🔍 Fokus 🗑 Beendet 📅 Geplant ⌵ Alle

Aktion	Beschreibung	Datum
✓	Konto-Mitgliedschaft verwalten CUSATUM\Hygienegruppe cusatumi@hygiene	Mo., 14.9.2026, 09:44
✓	Konto-Mitgliedschaft verwalten CUSATUM\Hygienegruppe cusatumi@hygiene	Fr., 11.9.2026, 14:09
✓	Konto-Mitgliedschaft verwalten CUSATUM\Gruppe Ute Testgroup cusatumi@hygiene	Fr., 4.9.2026, 19:20
⚠	Konto-Mitgliedschaft verwalten CUSATUM\Gruppe 2 cusatumi@hygiene	Fr., 4.9.2026, 19:15
✓	Konto-Mitgliedschaft verwalten CUSATUM\Gruppe llyl Testgroup cusatumi@hygiene	Fr., 4.9.2026, 19:09
⚠	Konto-Mitgliedschaft verwalten CUSATUM\Gruppe llyl Testgroup cusatumi@hygiene	Fr., 4.9.2026, 19:05
⚠	Konto-Mitgliedschaft verwalten CUSATUM\Gruppe llyl Testgroup cusatumi@hygiene	Fr., 4.9.2026, 19:04
✓	Konto-Mitgliedschaft verwalten CUSATUM\Gruppe llyl Testgroup cusatumi@hygiene	Fr., 4.9.2026, 19:03
✓	Konto-Mitgliedschaft verwalten CUSATUM\Brot_Bernd cusatumi@hygiene	Fr., 10.7.2026, 13:31
✓	Konto-Mitgliedschaft verwalten	Di., 8.6.2026, 18:35

Selektierte Verwaltungsaufgabe

Anzeige Status Löschen

✓ Konto-Mitgliedschaft verwalten
CUSATUM\Hygienegruppe
cusatumi@hygiene Mo., 14.9.2026, 09:44

Parameter	Wert
Gruppenmitglieder ändern (3)	
Mitglieder hinzufügen	CUSATUM\Christel Alber
Mitglieder entfernen	CUSATUM\Annaliese Butz CUSATUM\Carlheinz Hering CUSATUM\Christiana Abel
Kommentar	dfofsf
Gruppenmitgliedschaften ändern (?)	
Mitgliedschaften hinzufügen	
Mitgliedschaften entfernen	
Konto (1)	
Konto	CUSATUM\Hygienegruppe

Sie können konfigurieren, wie lange Sie Ihre Aufgaben in der CARO-Datenbank aufbewahren wollen. Gehen Sie dazu in den Konfigurationsmanager unter Globale Konfiguration\Datenbank\Richtlinien zur Datenaufbewahrung\Aufgabenausführungen:

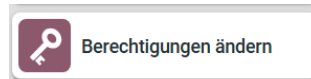
2 - 168



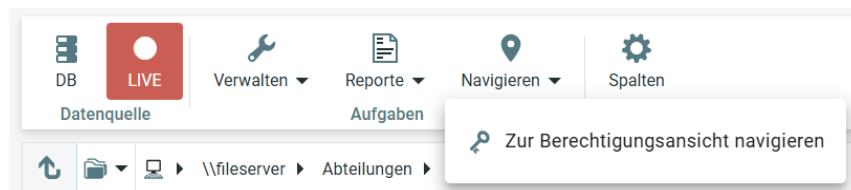
Berechtigungen ändern

Ansicht

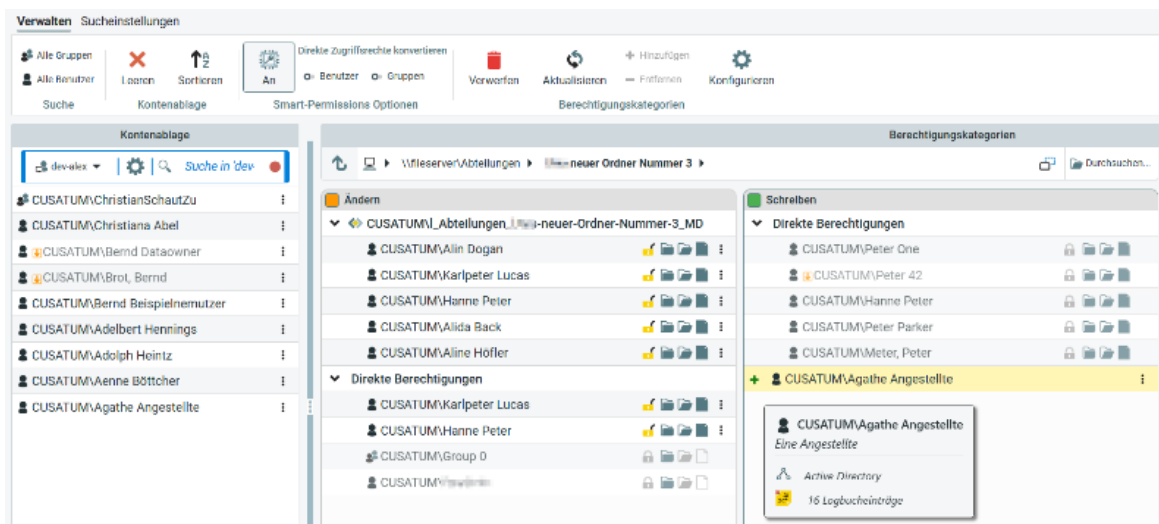
Die Berechtigungen ändern-Ansicht ist verfügbar über die Seitenleiste der CARO-Suite. In dieser Ansicht können Sie sich schnell einen Überblick über Ihre Berechtigungssituation verschaffen. Das Ändern von Berechtigungen über Drag&Drop ist ebenfalls möglich.



Tipp: Sie können über die Ressourcen-Ansicht im Live-Modus direkt zu Ihrem Verzeichnis navigieren:

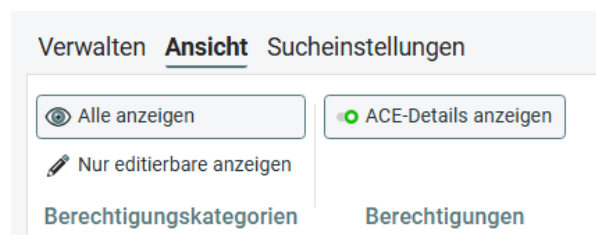


Unter Berechtigungen ändern sehen Sie alle Berechtigungen eines Verzeichnisses in übersichtlichen Kategorien.



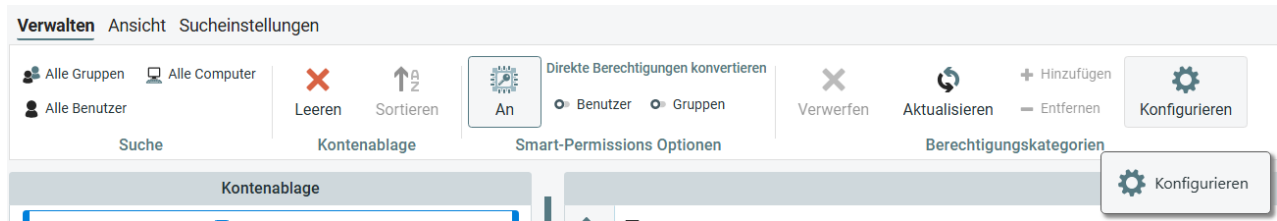
Anpassung der sichtbaren Kategorien

Die Kategorien können in der Globalen Konfiguration eingerichtet werden unter bearbeitbare Kategorien. In der Ansicht können Sie sich zusätzlich alle Kategorien anzeigen lassen, bzw. dies an oder abschalten. Gehen Sie dazu in das Untermenü Ansicht:

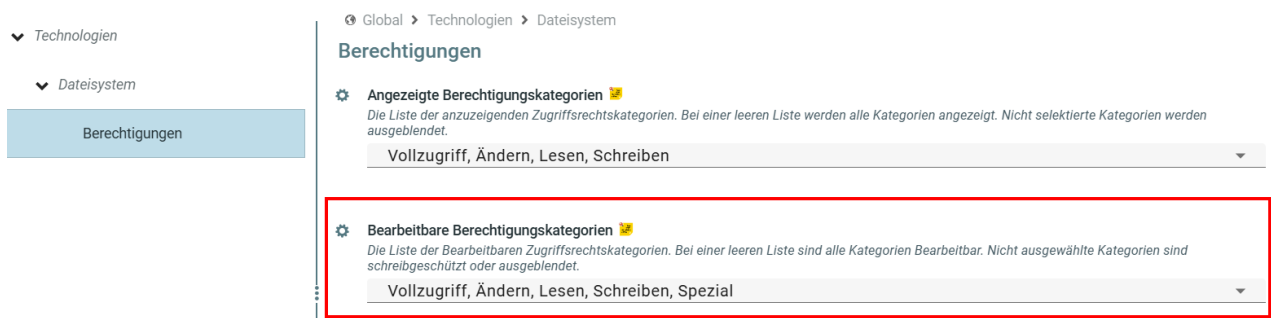




Über Konfigurieren im Verwalten Menü gelangen Sie direkt zu Globalen Einstellungen der Kategorien:

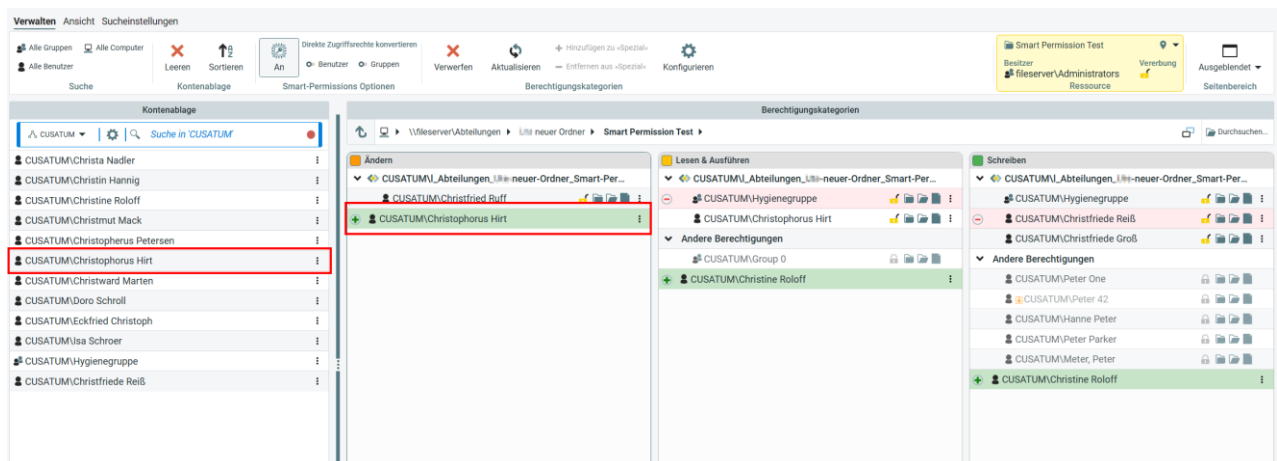


Die Globalen Einstellungen für Berechtigungskategorien:



Berechtigungsänderungen per Drag&Drop

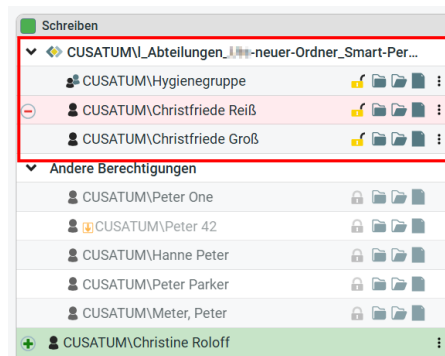
Änderungen sind schnell per Drag & Drop möglich. Nutzen Sie das automatische Erstellen von Berechtigungsgruppen dank **Smart-Permissions®**. Die Ansicht bietet Ihnen ebenfalls eine integrierte Kontenablage, um Ihre Konten einfach zu verwalten und schnell zu nutzen. Ziehen Sie Ihre Konten aus der Kontenablage direkt in Ihre gewünschte Berechtigungskategorie per Drag&Drop.



Smart Permissions® – Automatisch erzeugte Berechtigungsgruppen

Berechtigungen Sie Ihre Benutzer über vordefinierte Regeln, welche Sie pro Einstiegspunkt konfigurieren können. CARO erstellt dazu automatisch die passenden Berechtigungsgruppen oder nutzt vorhandene Gruppen.

CARO-Berechtigungsgruppen werden in den Kategorien als **CARO-Gruppen** identifiziert. Die Gruppenmitglieder werden innerhalb dieser Gruppen einsortiert:



Konten-Ansicht mit Suchfunktion

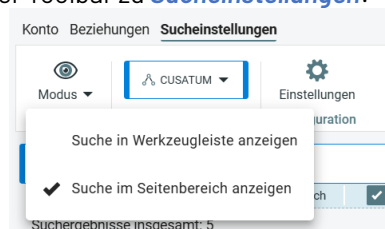
Diese Ansicht bietet Ihnen:

- Anzeige von Benutzer-, Gruppen- und Computerkonten für Ihre gescannten Domänen und lokalen File-server
- Übersicht über vorhandene Gruppenmitgliedschaften, direkte und indirekte Beziehungen, auch von verschachtelten Gruppen
- Anzeigen von Auffälligkeiten in der Berechtigungsstruktur des Active Directory
- Graphische Anzeige der Beziehungen zwischen Gruppen und Gruppenmitgliedern
- Schnelle, individuell einstellbare Suche von einzelnen Konten oder Inhalten von Konten-Eigenschaftsfeldern, dadurch einfache Überprüfung von firmenspezifischen Berechtigungskonzepten

Anzeigemodus wählen

In der Kontenansicht können Sie wählen, wie viel Bereiche Sie sehen wollen. Entweder 2 Bereiche: Selektion und das Seitenpanel für Details, oder 3 Bereiche: Suchpanel, Selektion und Seitenpanel rechts für Details.

Gehen Sie dazu in das Untermenü in der Toolbar zu **Sucheinstellungen**:





2 Bereiche - Suche ist in der Werkzeugleiste integriert

Name	Wert
accountexpires	Konto läuft nie ab
c	DE
cn	Aloys Böning
company	ACME Corp.
countrycode	0
department	Contracts
displayname	Aloys Böning
distinguishedname	CN=Aloys Böning,OU=UsersForTests,DC=cusatum,DC=de
employeeid	771571
givenname	Aloys
l	Bremen
mail	Aloys.Böning@cusatum.de
objectid	S-1-5-21-1031243688-930593761-1806467659-6681
postalcode	28309
primarygroup	513
pwdlastset	06/09/2020 14:45:14
samaccountname	Aloys.Böning
sn	Böning
st	Bremen
streetaddress	Hemmlinger Bahnhofstr 8
telephone	+49 421 170242
title	Clerk

3 Bereiche – Suchpanel im linken Bereich immer sichtbar

Name	Wert
accountexpires	Konto läuft nie ab
c	DE
cn	Aloys Böning
company	ACME Corp.
countrycode	0
department	Contracts
displayname	Aloys Böning
distinguishedname	CN=Aloys Böning,OU=UsersForTests,DC=cusatum,DC=de
employeeid	771571
givenname	Aloys
l	Bremen
mail	Aloys.Böning@cusatum.de
objectid	S-1-5-21-1031243688-930593761-1806467659-6681
postalcode	28309
primarygroup	513
pwdlastset	06/09/2020 14:45:14
samaccountname	Aloys.Böning

Suche konfigurieren

Mit der Suche können Sie Konten gezielt suchen. Standardmäßig wird immer nach dem Anzeigenamen gesucht. Sie können aber auch weitere Eigenschaften für die Suche hinzufügen. Ebenfalls können Sie wählen, wie der Suchstring gesucht werden soll: enthält, beginnt mit, endet mit oder ist genau gleich.

Einstellungen
Definieren Sie, in welchen Eigenschaftsfeldern die Suche durchgeführt werden soll

In diesem Beispiel wurden 2 Eigenschaften für die Suche konfiguriert:



Such-Einstellungen

Attribute (2) Starten der Suche

Wähle die Attribute aus, die für die Suche verwendet werden sollen. Der Kontoname (z.B. CUSATUM\Beate Burger) wird immer in die Suche einbezogen.

Filtern... 68 CUSATUM

Anzeigename	LDAP-Attributname
department	department
description	description
account-expires	accountexpires
address	streetaddress
carlicense	carlicense
comment	info
common-name	cn
company	company
country-code	countrycode

2 ausgewählte Suchattribute: department description Neu laden

Die Erweiterung der Suchkriterien um viele Attribute verlangsamt die Suche.

Schließen

CUSATUM chr 87 2 CUSATUM

enthält beginnt mit endet mit ist gleich

Suchergebnisse insgesamt: 87

Konto Mitgli... Eigenc...

2 Suchkriterien konfiguriert
department description

Sie können nun die gefundenen Konten einzeln selektieren, um sich die Details dazu anzuzeigen. In der Mitte wird das jeweils selektierte Konto aktualisiert:

CUSATUM chr 87 2 CUSATUM\Christfriede Groß

enthält beginnt mit endet mit ist gleich

Suchergebnisse insgesamt: 87

Konto	Mitgli...	Mitgli...	Eigenc...	Wert
CUSATUM\Andreas A...	10	departme	description	Wieder eine Bes...
CUSATUM\BGR_dev-fil...	2	descriptio	...ler01\TestData...	
CUSATUM\Chris Gregor	6	departme		
CUSATUM\Christa Nad...	2	departme		
CUSATUM\Christel Alber	3	departme		
CUSATUM\Christel Beh...	4	departme		
CUSATUM\Christfried ...	3	departme		
CUSATUM\Christfriede...	4	departme		
CUSATUM\Christfriede...	3	departme		
CUSATUM\Christhart J...	2	departme		
CUSATUM\Christhelm ...	1	departme		
CUSATUM\Christhelm ...	2	departme		
CUSATUM\Christhild BL...	4	departme		
CUSATUM\Christhild D...	3	departme		
CUSATUM\Christhild G...	1	departme		
CUSATUM\Christian C...	6	departme		

LDAP://CN=Christfriede Groß,OU=UsersForTests,DC=cusatum,DC=de

Active Directory 27.2.2026, 18:29:24

Zurück Vor Mitgliedschaft ändern Verwalten Reporte Navigieren

Graph Direkt Mitglied in

Eltern-Beziehungen

4

CUSATUM\Christfriede Groß
cusatum.de

Excel-Kontenreport erzeugen

Für jedes Konto können Sie einen Excel-Export aller Eigenschaftsfelder starten. Gehen Sie dazu auf die Schaltfläche **Export Excel** in der Eigenschaften-Ansicht.

Mitgliedschaftsbeziehungen darstellen

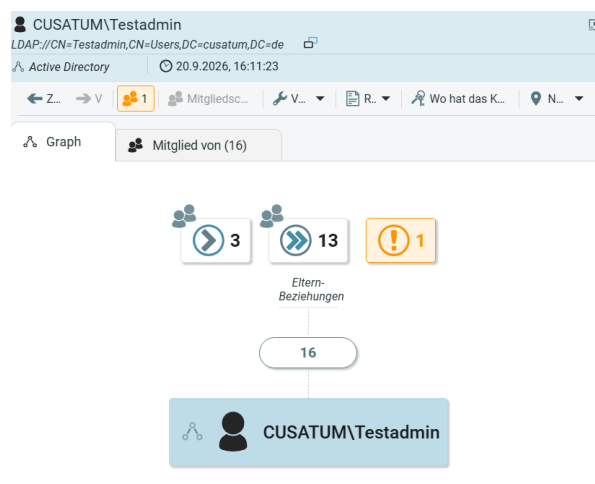
Für jedes Konto werden die Gruppenmitglieder („Kinder“, bei einer Gruppe) und die Gruppenbeziehungen („Eltern“) angezeigt. Sie sehen sofort, ob es direkte, oder auch indirekte Gruppenmitgliedschaften gibt.



Falls es Auffälligkeiten an einem Konto gibt, z.B. das Konto ist direkt und indirekt in einer Gruppe Mitglied, oder das Konto ist doppelt in der Gruppe enthalten, dann wird diese durch CARO mit einem Warnungs-Indikator



angezeigt:



Im rechten Seitenbereich unter **Beziehungen** können Sie sich die Details dazu ansehen.

Konto	Größe	LDAP-Container	Direkt	Indirekt	Ebenen
CUSATUM\Administrators	31	Built-in		1	3
CUSATUM\Denied RODC Password Replicatio...	32	Users		1	3
CUSATUM\Domain Admins	7	Users	✓		2
CUSATUM\Domain Users	8	Users	✓		1
CUSATUM\Event Log Readers	23	Built-in		1	3
CUSATUM\CompanyShare_Folder_A_mx	22.490	Fileserver		1	3
CUSATUM\Testshare_bb_Geda_IT_PDF Sca...	1	Fileserver		1	3
CUSATUM\Testshare_bb_Geda_ist	22.491	Fileserver		1	4
CUSATUM\Remote Desktop Users	22.491	Built-in		2	3
CUSATUM\Users	22.492	Built-in		1	3

Graphische Anzeige der direkten und indirekten Pfade

Die graphische Ansicht **Beziehungen** im Seitenbereich rechts visualisiert direkte und indirekte Beziehungen zwischen Benutzern und Gruppen.

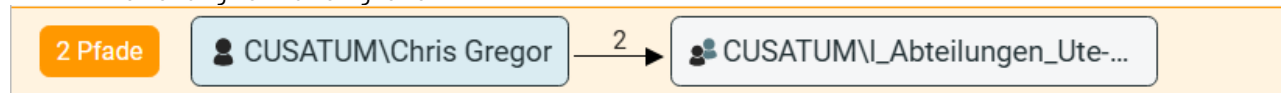


Bei den Pfad-Beziehungen der Gruppenmitgliedschaften gibt es 3 Stufen:

- Beziehung ohne Probleme



- Beziehung hat Auffälligkeiten



- Beziehung ist eine Rekursion



Gehen Sie dazu über die Mitgliedschaften-Liste. Sie sehen sofort, wo es in den Gruppenbeziehungen Auffälligkeiten gibt in der linken Spalte.

CUSATUM\Chris Gregor
LDAP://CN=Chris Gregor,OU=UsersForTests,DC=cusatum,DC=de
Active Directory 5 Logbucheinträge 18.9.2026, 10:16:01

Zurück Vor 2 Mitglieder ändern Verwalten Reporte Wo hat das Konto Zugriff? Navigieren

Graph Mitglied von (26)

Filtern...

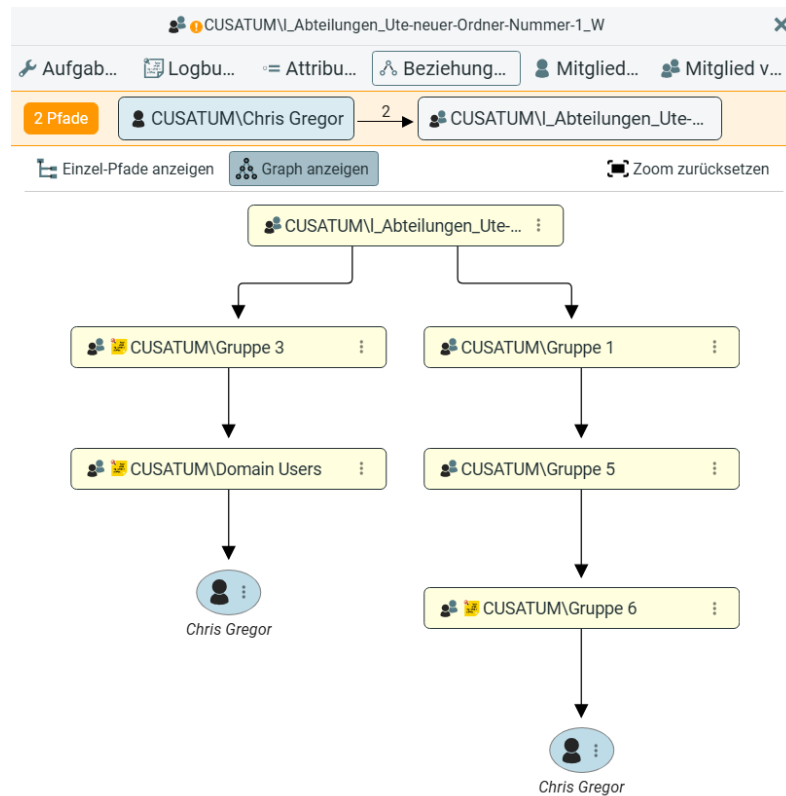
Alle Direkt Indirekt Mehrfach Auffälligkeiten

Konto			LDAP-Container	Direkt	Indirekt	Ebene
CUSATUM\Gruppe 6	5	22	Testgroups	✓		2
CUSATUM\Gruppe 13 Testgroup		13	Testgroups	✓		2
CUSATUM\CompanyShare_Folder A_mx		22.485	fileservers		1	3
CUSATUM\Testshare_bb_Geda_IT_PDF Scan_mx	1	22.485	fileservers		1	3
CUSATUM\I_Abteilungen_New-Folder-Ute-Neuer-Ordner-N...		3	fileservers	✓		2
CUSATUM\I_Abteilungen_Ute-Neuer-Ordner-N...		22.494	Caro-Berechtigungsgruppen		2	5
CUSATUM\I_Abteilungen_Ute-Neuer-Ordner-N...	5		fileservers	✓		2
CUSATUM\File-Server_Abteilungen_GF-2026_M-	9		fileservers	✓		2
CUSATUM\Finanz_Gehälter_Berlin_W	3		fileservers	✓		2
CUSATUM\I_TestOrdner_SP-Test_FC	1	4	Caro-Berechtigungsgruppen	✓	1	5
CUSATUM\I_Tests_W		1	Caro-Berechtigungsgruppen	✓		2
CUSATUM\Testshare_Ute-Neuer-Ordner-N...		31	Caro-Berechtigungsgruppen		1	5

Beziehung ist auffällig

CUSATUM\I_Abteilungen_Ute-Neuer-Ordner-N...		22.494	Caro-Berechtigungsgruppen		2	5
--	--	--------	---------------------------	--	---	---

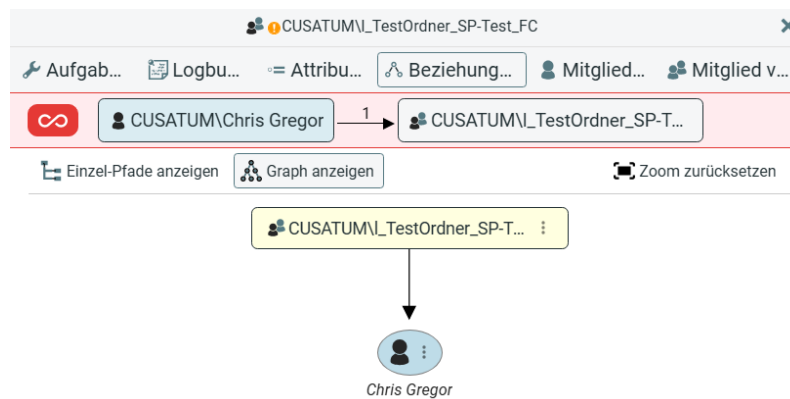
Das Konto Chris Gregor ist hier über 2 Wege in der Berechtigungsgruppe enthalten.



Beziehung mit Rekursion

!	CUSATUM\TestOrdner_SP-Test_FC	:	1	4	Caro-Berechtigungsgruppen	✓	1	∞
---	-------------------------------	---	---	---	---------------------------	---	---	---

Es wurde eine Rekursion erkannt: Chris Gregor ist in einer Rekursionsgruppe enthalten.



Wenn man sich diese Gruppe anzeigen lässt, erkennt man, sie enthält sich selbst als Mitglied:



CUSATUM\TestOrdner_SP-Test_FC
LDAP://CN=L_TestOrdner_SP-Test_FC,OU=Caro-Berechtigungsgruppen,DC=cusatum,DC=de
Write access group for '\\dev-lennart\TestOrdner\SP-Test' with object reference id '8b19cd9a-5ac3-4c1a-87c8-2ea2453d19cf'.
Active Directory 18.9.2026, 10:16:01

Zurück Vor 1 4 Mitgliedschaft ändern Verwalten Reporte Wo hat das Konto Zugriff? Navigieren

Graph Mitglieder (4) Mitglied von (1)

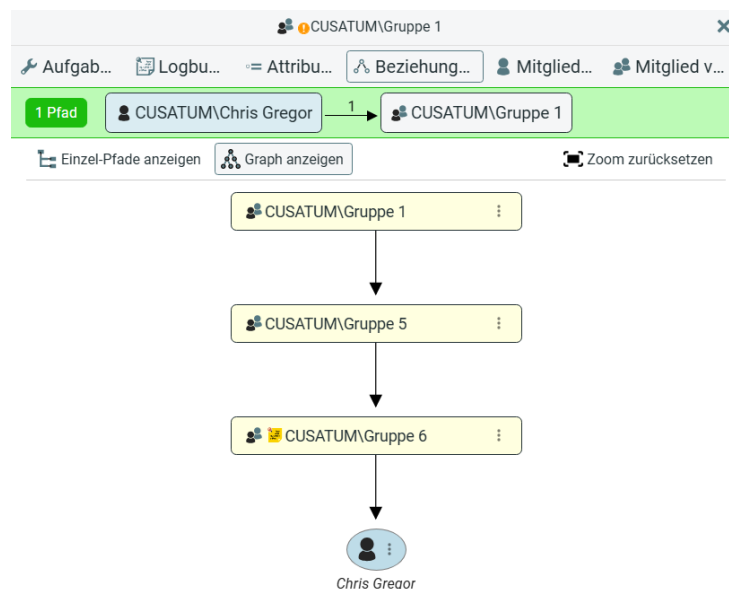
Filtern...

Alle Direkt Indirekt Mehrfach Auffälligkeiten

Konto			LDAP-Container	Direkt	Indirekt	Ebene
CUSATUM\Chris Gregor	26		UsersForTests	✓	1	
CUSATUM\Christa Nadler	17		UsersForTests	✓	1	
CUSATUM\Christel Alber	20		UsersForTests	✓	1	
CUSATUM\TestOrdner_SP-Test_FC	1	4	Caro-Berechtigungsgruppen	✓	1	

Zugriffspfade ohne Beanstandung

Lineare Gruppenbeziehungen, auch indirekte Beziehungen, werden im Seitenbereich grün dargestellt:



Globales Logbuch

Im Globalen Logbuch werden Änderungen zentral dokumentiert und sind jederzeit nachvollziehbar. Das Globale Logbuch sammelt alle von CARO erfassten Ereignisse – einschließlich der Observer-Events – zentral an einer Stelle. Über Filter nach Zeit, Autor oder einer bestimmten Ticket-ID finden Sie die gesuchten Informationen innerhalb weniger Sekunden.

Gründe für die Nutzung

- Dokumentationspflicht nachkommen
- Auffälligkeiten einfach überprüfen
- Überblick über ausgeführte Aktionen gewinnen



Quellen

Im Globalen Logbuch werden Ereignisse aus unterschiedlichen Quellen angezeigt.

Typ	Details
Konfiguration	Änderungen an Einstiegspunkten, Zugangskonten, Globale Einstellungen oder Smart-Permissions
Bereinigung	Bereinigungen, die automatisch oder manuell durchgeführt wurden
Verwalten	Alle ausgeführten Verwaltungsaktionen innerhalb der CARO-Suite
Observer	Automatisch aufgezeichnete Aktionen
Manuell	Von Anwendern manuell hinzugefügte Kommentare

Details – Was wird angezeigt

Für jeden selektierten Eintrag sehen Sie in den Details auf der rechten Seite:

- Typ: Über welche Quelle wurde eine Aktion ausgeführt
- Datum: Wann wurde die Aktion getätigt
- Autor: Wer war der Verantwortliche
- Kommentar: Was hat der Verantwortliche zu der ausgeführten Aktion kommentiert
- Bei Änderungen sehen Sie alle Objekte, z.B. Konten oder Verzeichnisse. Sie können direkt zu den Konten in die Kontenansicht navigieren oder bei Verzeichnissen die Ressourcenansicht öffnen.

Filtern nach Zeiträumen

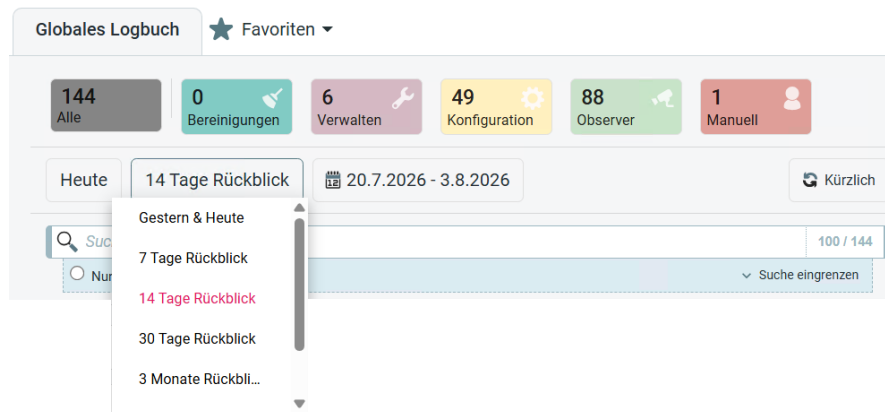
Setzen Sie explizit Zeiträume, welche Ereignisse Sie im Globalen Logbuch sehen möchten:

- Tagesaktuell





- Benutzerdefinierter Zeitraum
- vordefinierte Zeiträume



Suche

Suchzeile

Durchsucht die Kommentare nach Namen, Ressourcen, Ticketnummern oder ähnlichem.

Suche nach Autor

- Alle (Ungefiltert): sucht nach allen Einträgen ohne Einschränkung des Autors
- Nur meine: sucht ausschließlich nach Einträgen, die der aktuell eingeloggte Benutzer ausgeführt hat
- Nach Autor suchen: sucht ausschließlich nach Einträgen, die vom angegebenen Autor stammen

Suche nach Konten

Grenzen Sie Ihre Suche ein, z.B., um nach bestimmten Konten zu suchen, an den Änderungen durchgeführt wurden.

25

Suche nach Autor

☒ Alle
 ☐ Nur meine
 ☐ Nach Autor filtern

Suche nach Konto

Suche nach Ressource

In der Ergebnisliste sehen Sie alle gefilterten Änderungen am Objekt, hier die **Hygienegruppe**:

Typ	Erstellt	Kommentar	Autor
	14.09.2026, 09:45	Gruppenmitglied entfernt: Das Mitglied 'Annaliese Butz' wurde aus der globalen Sicherheitsgruppe 'Hygienegruppe' auf DC 'cusatum.de' entfernt (Datensatz:...	CUSATUM
	14.09.2026, 09:45	Gruppenmitglied entfernt: Das Mitglied 'Carlheinz Hering' wurde aus der globalen Sicherheitsgruppe 'Hygienegruppe' auf DC 'cusatum.de' entfernt (Datensatz:...	CUSATUM
	14.09.2026, 09:45	Gruppenmitglied entfernt: Das Mitglied 'Christiana Abel' wurde aus der globalen Sicherheitsgruppe 'Hygienegruppe' auf DC 'cusatum.de' entfernt (Datensatz:...	CUSATUM
	14.09.2026, 09:45	Gruppenmitglied hinzugefügt: Das Mitglied 'Christel Alber' wurde der globalen Sicherheitsgruppe 'Hygienegruppe' auf DC 'cusatum.de' hinzugefügt...	CUSATUM
	14.09.2026, 09:45	Gruppenmitglied entfernt: Das Mitglied 'Annaliese Butz' wurde aus der globalen Sicherheitsgruppe 'Hygienegruppe' auf DC 'cusatum.de' entfernt (Datensatz:...	CUSATUM
	14.09.2026, 09:45	Gruppenmitglied entfernt: Das Mitglied 'Carlheinz Hering' wurde aus der globalen Sicherheitsgruppe 'Hygienegruppe' auf DC 'cusatum.de' entfernt (Datensatz:...	CUSATUM
	14.09.2026, 09:45	Gruppenmitglied entfernt: Das Mitglied 'Christiana Abel' wurde aus der globalen Sicherheitsgruppe 'Hygienegruppe' auf DC 'cusatum.de' entfernt (Datensatz:...	CUSATUM



Suche nach Ressourcen

Die Angabe einer Ressource reduziert die Ergebnisse auf alle Einträge, die von ausgeführten Aktionen betroffen waren. Z.B. werden alle Änderungen an einer Ressource angezeigt, wo CARO-Berechtigungsänderungen durchgeführt hat.

5

Suche nach Autor

☒ Alle
 ☐ Nur meine
 ☐ Nach Autor filtern

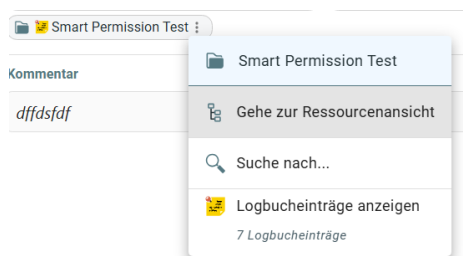
Suche nach Konto

Suche nach Ressource

Typ	Erstellt	Kommentar	Autor
	14.09.2026, 14:09	ich soll jetzt was machen	cusatum\useradmin
	14.09.2026, 09:46	dffdsfdf	cusatum\useradmin
	11.09.2026, 14:30	erzeuge eine leere Berechtigungsgruppe als Test	cusatum\useradmin
	11.09.2026, 14:25	ganz viele Änderungen	cusatum\useradmin
	04.09.2026, 13:48	Test auf langen Ordernamen	cusatum\useradmin

Weitere Funktionen

- Navigation zu einem Konto in die Kontenansicht
- Navigation zu einem Verzeichnis in die Ressourcenansicht
- Schnellsuche starten für Autor, Konto oder Ressource
- Anzeige der Logbucheinträge in einem Dialog für Objekte unter Details



- Export der Einträge in Excel

	A	B	C	D
1	Typ	Erstellt	Benutzerkommentar	Autor
2	Änderung	Mo., 14.9.2026, 14:09	ich soll jetzt was machen	cusatum\useradmin
3	Änderung	Mo., 14.9.2026, 09:46	dffdsfdf	cusatum\useradmin
4	Änderung	Fr., 11.9.2026, 14:30	erzeuge eine leere Berechtigungsgruppe als Test	cusatum\useradmin
5	Änderung	Fr., 11.9.2026, 14:25	ganz viele Änderungen	cusatum\useradmin
6	Änderung	Fr., 4.9.2026, 13:48	Test auf langen Ordernamen	cusatum\useradmin
7				

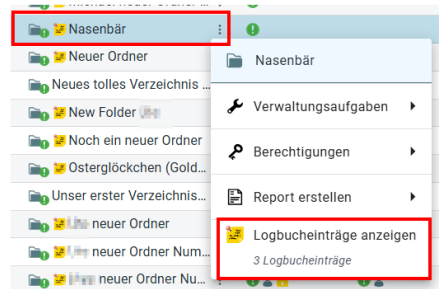
Logbucheinträge an Objekten

Jedes Objekt in der CARO-Suite kann eigene Einträge in einem Logbuch enthalten. Dies können z.B. Änderungen an einem Benutzerkonto sein, oder Konfigurationsänderungen an einem Einstiegspunkt. In allen Views und Listen können Sie das Logbuch über das Kontextmenü des Objekts aufrufen:

- Active Directory-Objekte, z.B. Benutzerkonten oder OU-Container

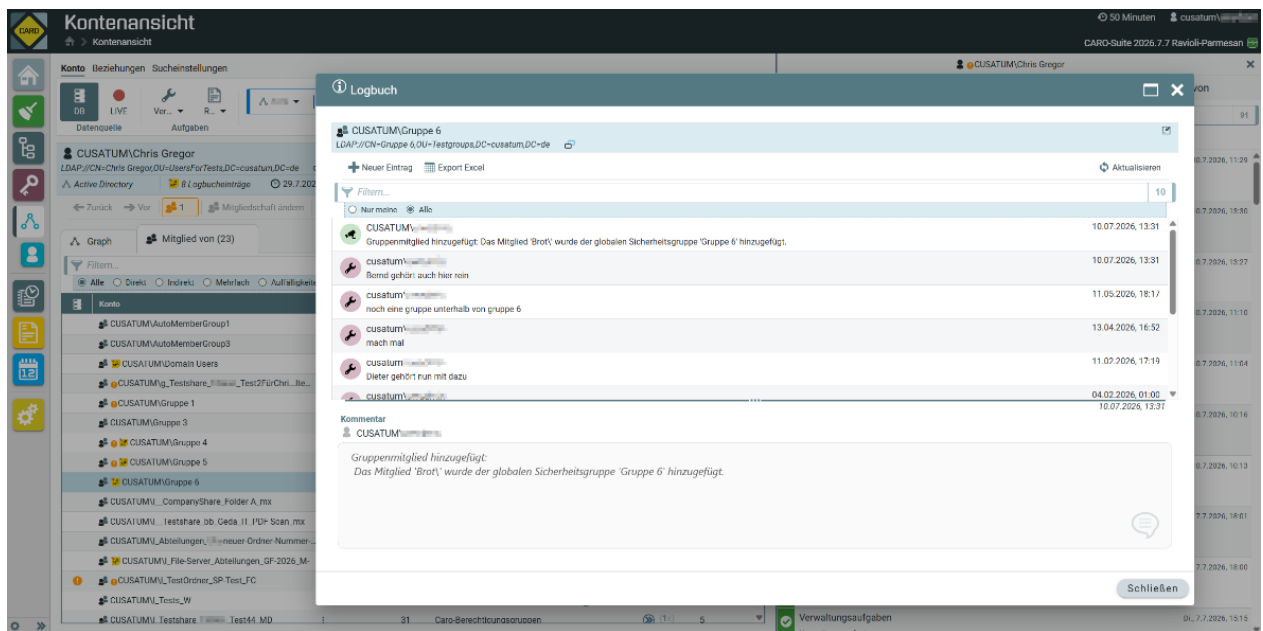


- Verzeichnisse
- Einstiegspunkte
- Konfigurationseinträge in der globalen Konfiguration



Die Logbuch-Einträge an jedem Objekt dokumentieren jede CARO-Änderung lückenlos:

- Perfekte Vorbereitung für Ihr nächstes Audit
- Nachvollziehbarkeit aller Änderungen
- Schnelle Identifikation von ungewollten Berechtigungsänderungen





CUSATUM Service GmbH

Mit über 25 Jahren Erfahrung im Berechtigungsmanagement und der Automatisierung von Mitarbeiterprozessen sind wir seit 2017 als eigenständiges Unternehmen für unsere Kunden da.

Unser Ziel: Ordnung ins Berechtigungschaos bringen!



Mit unserer CARO-Suite, dem CUSATUM Access Rights Optimizer, bieten wir eine smarte Lösung für automatisiertes Berechtigungsmanagement, mit der Sie Daten- und Zugriffsrechte schnell, sicher und automatisiert managen können.

Kurz gesagt: Weniger Klicks, weniger Chaos, mehr Sicherheit.

Herausgeber

CUSATUM Service GmbH

Wiesenweg 16

16548 Glienicke / Nordbahn

www.cusatum.de

info@cusatum.de



Support

+49 3305 678 3090

support@cusatum.de

In vielen Unternehmen kämpfen IT-Administratoren mit zeitfressenden Prozessen, um Zugriffsrechte zu vergeben. Deswegen haben wir die CARO-Suite entwickelt, die das Berechtigungsmanagement automatisiert und sowohl schneller als auch sicherer macht.

IT-Admins reduzieren damit den Aufwand, sichern die Kontrolle der Zugriffsrechte und vermeiden Sicherheitsrisiken für das Unternehmen.

Berlin, 20. September 2026