



Version 2024.8

Handbuch

Benutzerhandbuch der CARO-Suite





Inhaltsverzeichnis

Inhaltsverzeichnis	2
Installation und Konfiguration.....	4
Systemvoraussetzungen.....	4
Einfache Installation und Inbetriebnahme.....	4
CARO-Suite - WebClient	4
Start-Bildschirm	5
Konfigurationsmanager	6
Zugangskonten konfigurieren.....	6
Neue Anmeldung erstellen.....	7
Einstiegspunkte konfigurieren	7
Filesystem-Einstiegspunkte.....	8
Microsoft Entra ID Anbindung	13
Active Directory Einstiegspunkte.....	14
Benutzereinstellungen.....	14
Vorschaufeatures.....	15
Analyse- und Bereinigungsbausteine.....	16
Die Bausteine und ihre Anwendungsfälle.....	16
Best Practices	20
Das CARO-Dashboard	21
Default-Dashboard	21
Dashboard bearbeiten	21
Widget-Größe ändern	22
Ein neues Widget hinzufügen.....	23
Ein neues Dashboard erzeugen	24
Die Widgets und ihre Funktion	25
Neue Bereinigung: In 5 Schritten Ihr System bereinigen.....	30
Einen Scan konfigurieren	30
Risikobewertung und Analyse	32
Bewerten der Probleme.....	37
Bereinigen	38
Dokumentieren	38
Scan und Analysen wiederkehrend planen	40
Scans wiederkehrend planen.....	40
Auf einer bestehenden Analyse aufsetzen	41
Was sind „Elemente aus gelöschten Analysen“?	42



Weiter Aufräumen nach einer durchgeführten Analyse	43
Nach einigen Bereinigungen weiter aufräumen	43
Reporte anzeigen oder herunterladen	43
Automatisches Bereinigen mit der CARO-Suite	44
Fortschritts-Anzeige	44
Konfiguration	44
Bei Bewertungsvorschau anhalten (nur Bewerten)	45
Speicherbedarf minimieren	47
Ergebnisse	47
Ressourcen-Ansicht zur Berechtigungsanalyse	48
Berechtigungsreporte erstellen	49
Von einem Konto in die Kontenansicht navigieren	49
Eine IST-Berechtigungsanalyse starten	50
Anzeige von Berechtigungs-Anomalien	52
Verteilung von Berechtigungen (Statistiken)	52
Anzeige der Gruppenmitglieder	54
Filter für schnelles Auffinden von Mehrfach-Berechtigungen	55
Berechtigungs-Reporte	55
Erstellen von umfangreichen Reporten	59
Konten-Ansicht mit Suchfunktion	59
Durch das Active Directory navigieren	59
Suche konfigurieren	60
Eine Kontext-Suche für eine bestimmte Eigenschaft starten	61
Excel-Kontenreport erzeugen	61
Mitgliedschaftsbeziehungen darstellen	62
CUSATUM Service GmbH	63
Herausgeber	63
Support	63



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

Ein Video verdeutlicht, wie einfach die Installation und Inbetriebnahme der CARO-Suite ist. Sie erreichen erste Ergebnisse in weniger als 10 Minuten.

<https://youtu.be/FGMPERQQRNk>

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.

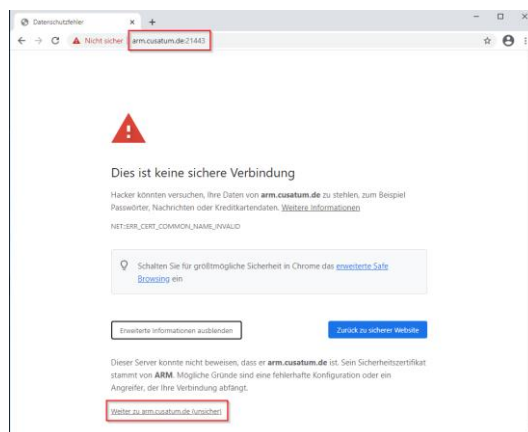
Diese Themen werden ausführlich behandelt:

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

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>**.

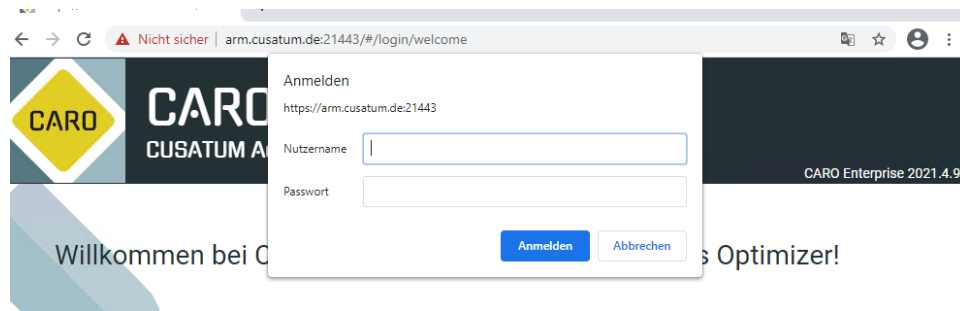
Wenn ein Self-Sign-Zertifikat benutzt wurde, dann muss das „Risiko“ akzeptiert werden.




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 eingetrag 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:


CARO-Suite
 CUSATUM Access Rights Optimizer
 Version 2022.12.16 (Muffin-Development)

Lizenzinformationen

Ausgestellt	9.12.2022, 09:03:05 (CUSATUM Service GmbH)
Lizenznehmer	CUSATUM Service GmbH
Lizenzzeitraum	Von Fr., 9.12.2022, 11:34 bis Mo., 8.1.2024, 11:34
Maintenance	Unbefristet

 Ihre Lizenz ist gültig.

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

- Scan konfigurieren**
 - Einstiegspunkte und ihre Scan-Parameter einrichten
 - Anmeldedaten zum Scannen und Ändern eingeben
 - Aufgabe für eine Bereinigung auswählen
- Analysieren und Bewerten der Berechtigungsprobleme**
 - CARO zeigt nach dem Scan alle Berechtigungsprobleme auf, wo sich unaufgelöste Berechtigungseinträge oder verwaiste Besitzer befinden
- 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.

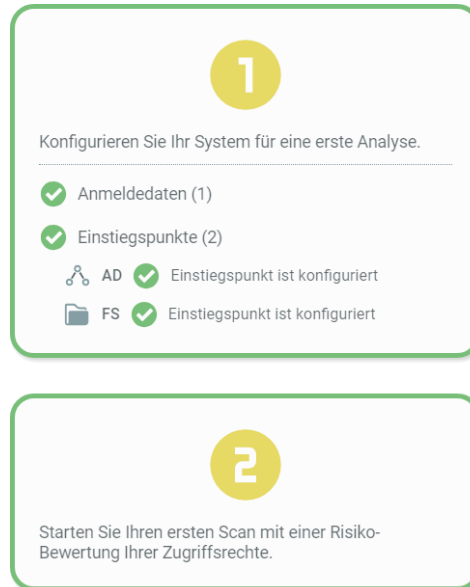
- Es wurden noch keine Anmeldedaten konfiguriert.
- Es wurden noch keine Einstiegspunkte konfiguriert.

2
 Starten Sie Ihren ersten Scan mit einer Risiko-Bewertung Ihrer Zugriffsrechte.





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 [Einen Scan konfigurieren](#).



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.





Neue Anmeldung erstellen

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



Konfigurieren Sie die Anmeldedaten zum erfolgreichen Scannen und Bereinigen Ihrer Systeme.

Neue Anmeldung erstellen



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.

Einstiegspunkt erstellen

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

- 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.

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

Ressource auswählen

Anmeldedaten

XXXXXXXXXXXX

MyVmware\TestData

Ressourcen

Ressourcen unterhalb von 'TestData' filtern...

2

Name

..

scripts

Ressource ausgewählt

Auswählen

Abbrechen



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 Ressource-Ansicht im Baum angezeigt:

⚙	Name	Scan-Zeit	Auffälligkeiten hier	Auffälligkeiten unterhalb	Verteilung der Berechtigungen
→	📁 C:\Users	15.6.2023, 14:23	🟢 👤	🟢 👤 🔒	<div><div></div><div></div><div></div></div>
→	📁 [Icon]	15.6.2023, 14:23	🟢 🔒	🟢 👤 🔒	<div><div></div><div></div><div></div></div>
→	📁 Test Marketing	15.6.2023, 14:23	🟢 👤	🟢 👤	<div><div></div><div></div><div></div></div>
→	📁 Department	15.6.2023, 14:23		🟢 👤	<div><div></div><div></div><div></div></div>
→	📁 Marketing 1	15.6.2023, 14:23		🟢 👤	<div><div></div><div></div><div></div></div>
→	📁 Raum 1	15.6.2023, 14:23	🟢 👤	🟢	<div><div></div><div></div><div></div></div>
→	📁 Ebene 5	15.6.2023, 14:23		🟢	<div><div></div><div></div><div></div></div>
.....					
↶	Kinder von 📁 Ebene 5				
	📁 Ebene 6	15.6.2023, 14:23	🟢		<div><div></div><div></div><div></div></div>



Beispiel für eine Speicherbegrenzung

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

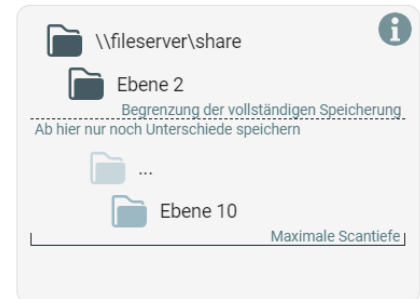
Scantiefeneinstellungen

Maximale Scantiefe

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

Begrenzung der vollständigen Speicherung

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.

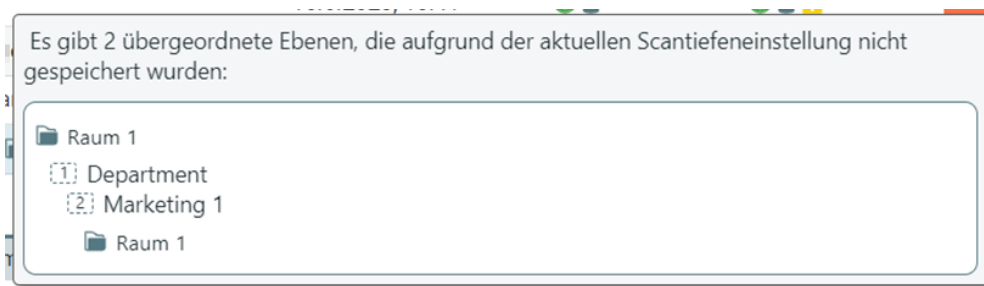


Anzeige in der Ressourcen-Ansicht

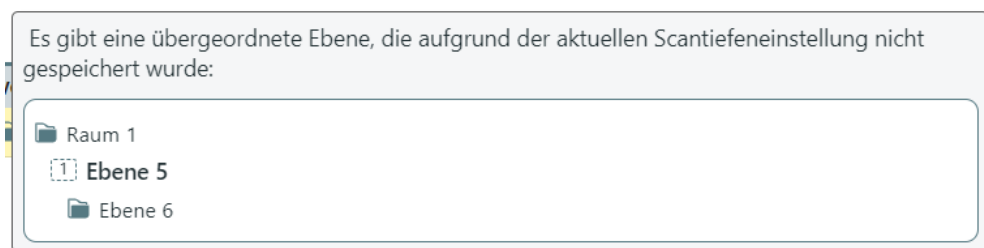
In der Ressourcenansicht werden alle Verzeichnis-Ebenen „dazwischen“ nicht mehr im Baum angezeigt. Im Tooltip oder über ein Kästchen am untergeordneten Verzeichnis sehen Sie, in welcher Ebene wieder ein Verzeichnis mit geänderter Berechtigungslage existiert. Dies wird wie gewohnt im Baum angezeigt:

🔧	Name	Scan-Zeit	Auffälligkeiten hier	Auffälligkeiten unterhalb	Verteilung der Berechtigungen
➔	📁 C:\Users	15.6.2023, 10:41	🟢 👤	🟢 👤 🔒	<div><div></div><div></div><div></div></div>
➔	📁 [unlesbar]	15.6.2023, 10:41	🟢 🔒	🟢 👤 🔒	<div><div></div><div></div><div></div></div>
➔	📁 Test Marketing	15.6.2023, 10:41	🟢 👤	🟢 👤	<div><div></div><div></div><div></div></div>
➔	📁 [2] 📁 Raum 1	15.6.2023, 10:41	🟢 👤	🟢	<div><div></div><div></div><div></div></div>
...					
🔄	Kinder von 📁 Raum 1				
	📁 Ebene 6	15.6.2023, 10:41	🟢		<div><div></div><div></div><div></div></div>

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



Alle Ebenen oberhalb von **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.

Einstiegspunkte

CARO Konfigurationsmanager > Einstiegspunkte

Active Directory | Microsoft Entra ID | **Filesystem** | Lokale Konten

Erstellen

Einstiegspunkte filtern... 5

Name	Uri	System	Anmeldedaten	Sonst. Einstellungen
dev-filer01	\\filer01	dev-filer01	cusaturnutzer001	Max. 10 Ebenen (8 vollst. speiche... Lokale Konten mitscannen
fileserv	\\fileserv	fileserv	cusaturnutzer001	Max. 10 Ebenen (8 vollst. speiche... Lokale Konten mitscannen
Abteilungen	\\fileserv\Abteilungen	fileserv	cusaturnutzer001	Max. 10 Ebenen (8 vollst. speiche... Lokale Konten mitscannen
Finanz	\\fileserv\Finanz	fileserv	cusaturnutzer001	Max. 10 Ebenen (8 vollst. speiche... Lokale Konten mitscannen
Test-Share_001	\\fileserv\TestShare_001	fileserv	cusaturnutzer001	Max. 10 Ebenen (8 vollst. speiche... Lokale Konten mitscannen



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 ebenfalls ein Video 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.

Wie möchten Sie die CARO-Anmeldung für EntraID erstellen?

Um auf Ihre EntraID-Ressourcen zugreifen zu können, benötigen Sie das Client Secret einer Anwendung mit entsprechenden Berechtigungen. Die CARO-Suite bietet Ihnen zwei Möglichkeiten, ein solches Client Secret als Credential zu konfigurieren: 1) Sie können entweder CARO automatisch eine passende App registrieren lassen und deren Client Secret als Anmeldung konfigurieren. 2) Oder Sie können Ihr eigenes Client Secret konfigurieren (z.B. wenn Sie bereits eine App für diesen Zweck registriert haben).

Ich habe noch kein Client-Secret

Es wird eine neue Anwendung registriert. Das Client-Secret dieser Anwendung wird Ihnen anschließend zum Speichern und/oder zum Konfigurieren als CARO-Anmeldung angeboten.

Ich besitze bereits ein Client-Secret

Konfigurieren Sie eine CARO-Anmeldung einfach durch Eingabe des Client-Secrets einer bestehenden Anwendung.

[Abbrechen](#)

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

Schritt 3: Anwendung registrieren

Für den Zugriff auf Ihre Azure-Ressourcen ist eine Anwendung mit ausreichenden Berechtigungen erforderlich. CARO registriert eine geeignete Anwendung automatisch unter Verwendung der Microsoft-Geräteautorisierungsgenehmigung und speichert das Client-Geheimnis als CARO-Anmeldeinformation.

1 Gerätecode anfordern 2 Autorisierung 3 Anwendung registrieren 4 CARO-Anmeldedaten erstellen

Anwendungsname (optional): Mein neuer CARO-M365 Connector

Anwendung wird registriert...

[< Zurück](#) [Registrieren >](#)

Nach erfolgreicher Prüfung auf der Mirosoft-Seite (Benutzercode: GUDPZXW6W), können Sie mit der Registrierung der Anwendung fortfahren.

[Abbrechen](#)

Schritt 4: CARO-Anmeldedaten erstellen

Für den Zugriff auf Ihre Azure-Ressourcen ist eine Anwendung mit ausreichenden Berechtigungen erforderlich. CARO registriert eine geeignete Anwendung automatisch unter Verwendung der Microsoft-Geräteautorisierungsgenehmigung und speichert das Client-Geheimnis als CARO-Anmeldeinformation.

1 Gerätecode anfordern 2 Autorisierung 3 Anwendung registrieren 4 CARO-Anmeldedaten erstellen

Tenant: cusatum.de
 ApplicationName: Mein neuer CARO-M365 Connector
 AppId: ef67d36c-853c-4ed8-9169-1346399d477d
 ClientSecret: UL18*****

[Erstellen >](#)

Anwendung wurde erfolgreich registriert. Bitte speichern Sie das angezeigte Clientgeheimnis in einem sicheren Ort. Klicken Sie auf 'Erstellen', um dieses als CARO-Anmeldung einzurichten.

[Abbrechen](#)

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

LDAP://DC=cusatum,DC=de

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

Derzeit sind 24 Attribute und 10 Objektklassen zum Scannen an- bzw. abwählbar.



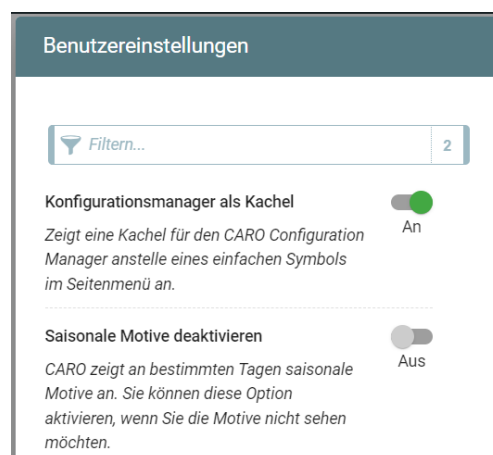
Hinweis: Eine doppelte Konfiguration von Domänen als Einstiegspunkte ist nicht möglich. Falls Sie dies trotzdem konfigurieren, wird die Speicherung einer doppelten Domäne mit einer Fehlermeldung abgebrochen. Der URL-Pfad der Domäne wird hier geprüft, ob er bereits verwendet wird. Mehrfachbenutzung von 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 mögliche Probleme analysiert. Lesen Sie mehr zu den verfügbaren Bausteinen und Best Practices zur Bereinigung im Kapitel **Analyse- und Bereinigungsbau- steine**.

Benutzereinstellungen

Ebenfalls können Sie saisonale Motive für Ihren Header einblenden. D.h. im Winter wird Ihre CARO-Suite Schneefall anzeigen. Lassen Sie sich überraschen, welche Motive es noch gibt.



Bei aktivierter Kachelansicht sehen Sie nun auch den Konfigurationsmanager in der Navigationsleiste:

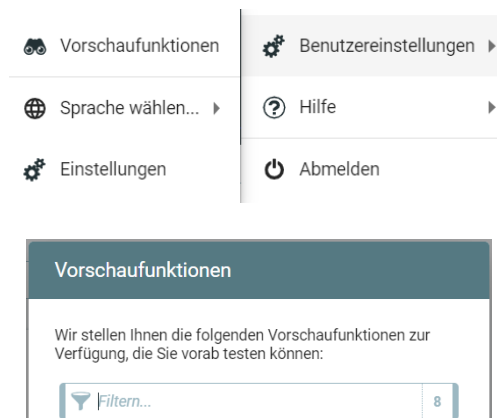


Vorschaufeatures

Ab der Version 2021.12 bieten wir ein neues Feature an: die CARO-Vorschaufunktion. Dadurch 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.

Freischalten der Vorschaufeatures

Die Vorschaufeatures müssen Sie im User-Menü unter **Benutzereinstellungen - Vorschaufunktionen** einmalig einschalten.





Analyse- und Bereinigungsbausteine

Die Bausteine und ihre Anwendungsfälle

Die CARO-Suite umfasst derzeit 12 Analyse- und Bereinigungsbausteine. Diese werden bei der Konfiguration des Scans Ihrer Einstiegspunkte angeboten. Für eine effiziente Grund-Bereinigung Ihrer IT-Systeme gibt es sinnvolle Kombinationen und eine empfohlene Reihenfolge der einzelnen Bausteine.

Im Kapitel [Best Practices](#) wird darauf genauer eingegangen.

BAKS



Besitzer-Analyse- und Korrektur-Software

- Stellt zulässige Besitzer sicher, damit administrative Konten Ihre Berechtigung behalten, z.B. damit Backup-Tools funktionieren
- Analysiert Sicherheitsrisiken durch das Entfernen von unerlaubten und unkontrollierbaren Zugriffs-Berechtigungen

Anwendungsfall: Durch das Erstellen von Verzeichnissen und Dateien bekommen „normale“ Benutzer das Besitzrecht. Dadurch sind diese Benutzer in der Lage, die Berechtigung selbst zu verändern. Im schlimmsten Fall werden hier die Administratoren, Service Accounts und Benutzer ausgesperrt. Best-Practice ist es, diese Benutzer durch die lokalen Fileserver-Administratoren auszutauschen.

Besitzer korrigieren



DARS



Direktzugriff Analyse- und Restrukturierungs-Software

- Identifiziert Direktberechtigungen von Usern
- Korrigiert effizient diese Einträge

Anwendungsfall: Wilma Gucken ist Mitglied in der Gruppe Finanzabteilung und hat zusätzlich direkten Zugriff auf Geschäftsdaten. Nachdem Wilma nicht mehr in der Finanzabteilung ist, hat sie trotzdem noch Zugriff! DARS findet schnell alle Gruppen- und direkten Benutzerzugriffe und löscht diese überflüssigen Zugriffsrechte effektiv. Für andere Benutzer mit direkten Zugriffsrechten werden Hinweise erzeugt.

Direkte Berechtigungen checken



TEUS



Tool zur Entfernung Unbekannter SIDs

- Entfernt tote SIDs und macht die Dokumentation Ihrer Berechtigungen wieder leichter lesbar und verständlich
- Reduziert die Nachfragen Ihrer Revision und dokumentiert, dass Sie die volle Kontrolle haben
- Bietet mehr Sicherheit, da weniger Angriffsfläche für SID History Injection

Anwendungsfall: Nach dem Löschen von Benutzern und Gruppen im Active Directory werden diese in den berechtigten Ressourcen-ACL's nicht automatisch mit entfernt. Zurück bleibt auf den Ressourcen die verwaiste oder tote SID. Diese Einträge machen notwendige Audit-Reporte

Unbekannte SIDs entfernen





EBIS



Erfassung der **B**erechtigungs-**I**ST-Situation

- Zeichnet die Berechtigungslage auf Fileservern und im Active Directory auf
- Analysiert u.a. auf unterbrochenen Vererbungshierarchien, verschobene Verzeichnisse oder Null-DACL
- Zeigt im Detail die geänderten Berechtigungen unterhalb an, wie hinzugekommene oder entfernte Zugriffsrechte

Anwendungsfall: Sie wollen regelmäßig Ihre Berechtigungen in der globalen Ressourcen-Ansicht überprüfen oder Berechtigungsreporte erstellen, wie Wer-hat-Wo-Zugriffs-Report, Use-Case-Report oder einen Berechtigungs-Differenz-Report.

IST-Situation erfassen und Berechtigungen reporten

LARS



Listgruppen **A**nalysen- und **R**estrukturierungs-**S**oftware

- Analyse der Berechtigungen in Ordner-Hierarchien
- Verwalten von List-Berechtigungen in übergeordneten Ordnern

Anwendungsfall: Benutzer sollen zu den „Arbeitsverzeichnissen“ navigieren können. Best-Practice sieht dafür eine Listberechtigung vor, die über Active Directory-Gruppen gesteuert wird. Durch die tägliche Arbeit werden oft Verzeichnisse verschoben, neu erstellt, umbenannt oder gelöscht. Dabei müssen die Listberechtigungen mit korrigiert werden, damit die Benutzer weiterhin problemlos zu den Verzeichnissen gelangen. Weder die Administratoren noch auf dem Markt befindliche Software z.B. SolarWinds-ARM, Tenfold oder IDM/IAM-Systeme korrigieren diese Probleme nachhaltig.

Fehler in Listgruppen analysieren



ERBE



Ersteller-**B**esitzer auf Dateisystemen **E**ntfernen

- Entfernt den Ersteller-Besitzer und verhindert das Entstehen von neuen toten SIDs
- Erlaubt damit eine saubere Migration, z.B. in die Cloud

Anwendungsfall: Standard-Einstellung von Microsoft beim Einbinden neuer Festplatten ist es, die Ersteller-Besitzer-Berechtigung mit Vollzugriff zu vergeben. Dadurch entstehen direkte Berechtigungen, die bei einem Löschen des Benutzers zu einer verwaisten SID führt. Zusätzlich kann der Benutzer die Administratoren, Service Accounts und Benutzer auszusperrern. Best-Practice von CUSATUM ist, diesen Eintrag zu entfernen und mit einer Gruppenberechtigung zu arbeiten.

Ersteller-Besitzer entfernen



DUKE



Direktzugriffsrechte **U**ngewollter **K**onten **E**ntfernen

- Identifiziert alle Zugriffsrechte der konfigurierten ungewollten Konten und entfernt diese
- Reduziert Sicherheitsrisiken durch das Entfernen von unbekannten und unkontrollierbaren Zugriffsberechtigungen

Anwendungsfall: Administratoren bekommen durch die UAC einen Vollzugriff gewährt. Mit DUKE werden diese direkten Einträge entfernt und die Gruppenmitgliedschaft über die Administratoren-Gruppe wird wieder hergestellt.

Direkte ungewollte Berechtigungen entfernen





SARA



Share Access Rights Analysis

Analyse von Freigabe-Zugriffsrechten

- Prüfen auf vererbte NTFS-Zugriffsrechte
- Suchen von **offenen Shares** für authentifizierte Konten
- Suchen von Jeder-Vollzugriff Freigaben
- Prüfen auf die Existenz von nicht-administrativen Freigaben

Anwendungsfälle:

- (1) 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.
- (2) Freigaben werden überprüft, ob authentifizierte Konten (AD und lokal) mindestens das Lese-Zugriffsrecht haben. Dann gelten diese Freigaben als **offene Shares**. Damit kann ein unkontrollierter Datenabfluss erfolgen.
- (3) 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.
- (4) Ihre Server werden auf die Existenz von nicht-administrativen Freigaben geprüft. Administrative Freigaben (C\$, etc.) werden dabei ignoriert. Freigaben können unkontrollierten Zugriff auf kritische Informationen ermöglichen.

Freigabe-Berechtigungen überprüfen



RAPA



Redundant Account Permission Analysis

- Identifiziert redundante Berechtigungen
- Überprüfen von Gruppenmitgliedschaften mit gleichzeitiger Direktberechtigung

Anwendungsfall: Wenn ein Benutzer eine direkte und eine gleichwertige oder höhere Gruppenberechtigung bekommen hat, ist die direkte Berechtigung redundant. In diesem Fall kann die direkte Berechtigung entfernt werden. Somit vermeidet man auch das verwaiste-SID-Problem und kann den Leaver-Prozess einfacher und effektiver gestalten.

Redundante Berechtigungen beseitigen



VASS



Vererbung-Analyse- und Sanierungs-Software

- Identifiziert veränderte Berechtigungen in Ordner-Hierarchien
- Findet verschobene Verzeichnisse
- Angleichung der Berechtigungen durch Vererbung oder andere system-spezifische Werkzeuge

Anwendungsfall: Das Aufbrechen von Vererbung unterhalb der zu administrierenden Verzeichnisebenen ist oft ungewollt und führt dazu, dass Benutzer dort nicht mehr zugreifen können. Best-Practice ist, dass nach der Administrationsebene alle Berechtigungen durchvererbt sind. CUSATUM empfiehlt maximal 4 Ebenen.

Aufgebrochene Vererbungen wiederherstellen,



Verschobene Verzeichnisse finden





MARS



Mindestberechtigungen Analyse und Restrukturierungs-Software

- Prüft alle Dokumente und Ordner auf erforderliche Zugriffsrechte für Konten und berücksichtigt dabei sowohl direkte als auch indirekte Zugriffsrechte
- Setzt fehlende Berechtigungen

Anwendungsfall: Sie wollen die Mindestberechtigung für einen Benutzer überprüfen, ob z.B. ein Benutzer oder ein Service Account überall mindestens Modify hat. Oft sind entweder keine Berechtigungen oder eine zu geringe Berechtigung vergeben.

Mindest-Berechtigungen überprüfen



ARCA

Account Risk- und Compliance-Assessment

- Analysiert Konto-basierend auf Best Practice-Kriterien
- Für Active Directory und Entra ID

Active Directory (AD)

- Inaktive Benutzer- oder Computerkonten
- Deaktivierte Benutzerkonten
- Leere Gruppen und Gruppen ohne Beschreibung
- Konten mit nie ablaufenden Kennwörtern

Anwendungsfall: Das BSI und andere IT-Auditierungen, wie TISAX und BAFIN, überprüfen sicherheitskritische KPIs im Active Directory. Dadurch kann die Qualität der Mitarbeiterprozesse und die IT-Sicherheit überprüft und gewährleistet werden. Im ARCA-Modul sind die wichtigsten AD-Analysen zusammengefasst und können individuell angepasst werden.

Entra ID – Zugriffsüberprüfungen in der Cloud

- Globale Administratoren auf zulässige Anzahl prüfen
- Anzahl der privilegierte Rollenzuweisungen überprüfen
- Ausschließliche Nutzung von Gruppen in Rollenzuweisungen
- Überprüfen, dass nur Cloud-native-Konten für Rollenzuweisungen genutzt werden
- Ablaufende Clientschlüssel in den App-Registrierungen finden
- Finden von inaktiven Gastbenutzern, die sich über einen längeren Zeitraum nicht angemeldet haben
- Auffinden aller inaktive Cloud-native Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind

Anwendungsfall: Mit CARO können Sie jetzt Ihre Zugriffe für cloudbasierte und hybride Ressourcen auf Entra ID überprüfen und bereinigen. CARO integriert dabei Best Practices für Microsoft Entra-Rollen*.

*Eine ausführliche Beschreibung der Microsoft Best Practices finden sie hier:
<https://learn.microsoft.com/de-de/entra/identity/role-based-access-control/best-practices>

Account Risk- und Compliance Analysen für Active Directory und Entra ID





Best Practices

Für das Bereinigen ist es sinnvoll, bestimmte Analysen gemeinsam zu nutzen. Sehen Sie in der folgenden Übersicht eine empfohlene **Reihenfolge** der CARO-Analysen für ein effizientes Scannen und Aufräumen.

Reihenfolge	Analyse-Bau- steine	Technologie	Sinnvolle Einstellung in der CARO-Suite
1 Domänen-Scan als Grundvoraussetzung	ARCA	AD, Entra ID	Täglich scannen, Mindestens inaktive Benutzer suchen
2 Freigabe-Berechtigungen überprüfen	SARA	FS	Mindestens 1x pro Woche
3 Tote SIDs finden und entfernen	TEUS	FS, AD	Mindestens 1x pro Woche
4 Besitzer korrigieren	BAKS	AD, FS	*Damit ggf. die durch CREATOR_ONWER erzeugten Direktberechtigungen durch spätere ERBE-Bereinigungen bestehen bleiben.
5 Direkte Berechtigungen aufräumen	DARS	FS	
6 Problematische Ersteller-Besitzer korrigieren	BAKS DARS ERBE	FS	*Darf laufen, wenn BAKS gelaufen ist ODER auf dem System ein Gruppenkonzept eingesetzt wird UND DARS keine Hinweise liefert, d.h. es fehlen keine Berechtigungsgruppen.
7 Direkte ungewollte Berechtigungen entfernen	DUKE	FS, AD	
8 Redundante Berechtigungen beseitigen	RAPA	FS	
9 Mindest-Berechtigungen überprüfen und korrigieren	MARS	FS	



<p>10</p> <p>Unterbrochene Vererbungen finden und beseitigen, Verschobene Verzeichnisse finden und korrigieren</p>	<p>VASS</p>	<p>FS</p>	<p>Immer am Ende der Aufräumprozesse durchführen.</p>
<p>Listberechtigungen überprüfen</p>	<p>LARS</p>	<p>FS </p>	<p>Immer am Ende der Aufräumprozesse durchführen.</p>

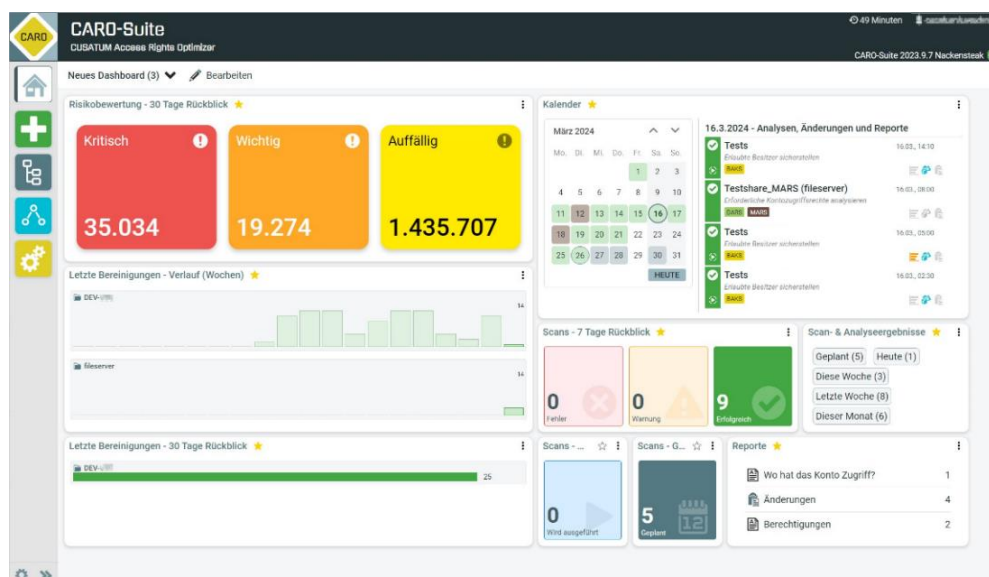
- wird derzeit nur als Audit-Baustein angeboten

Das CARO-Dashboard

Default-Dashboard

Auf der Homepage 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.



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:

CARO-Dashboard



Speichern



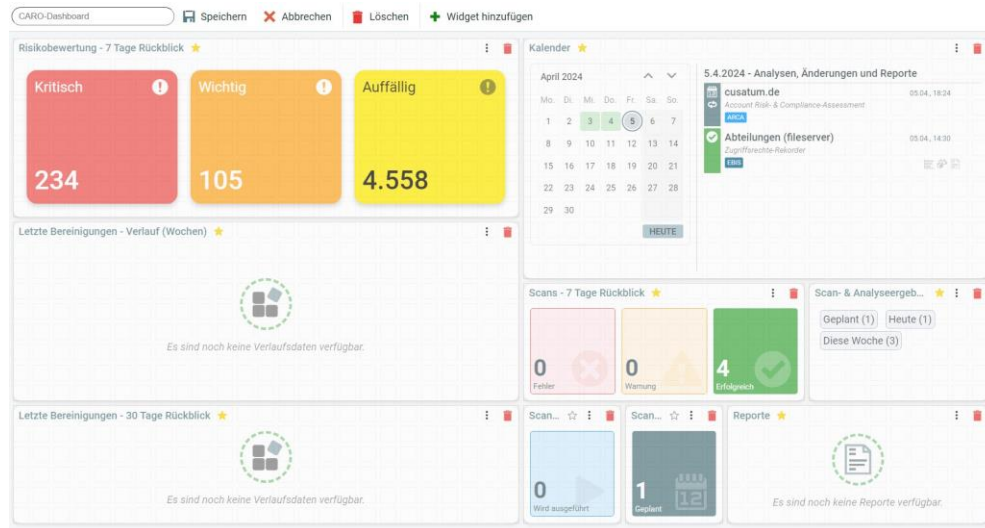
Abbrechen



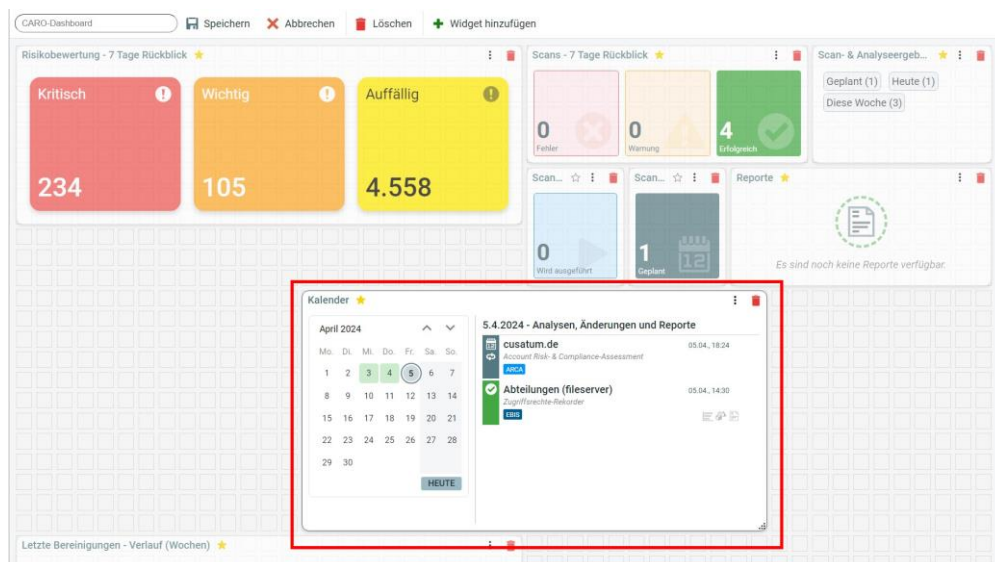
Löschen



Widget hinzufügen



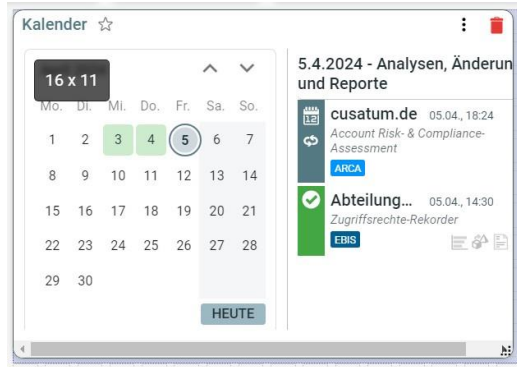
Die einzelnen Widgets sind nun verschiebbar oder löschtbar. Zum Verschieben einfach mit der Maus ein Widget „greifen“ bzw. anklicken und dann an die gewünschte neue Position verschieben. Die anderen Widgets positionieren sich automatisch in neue freie Flächen.



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

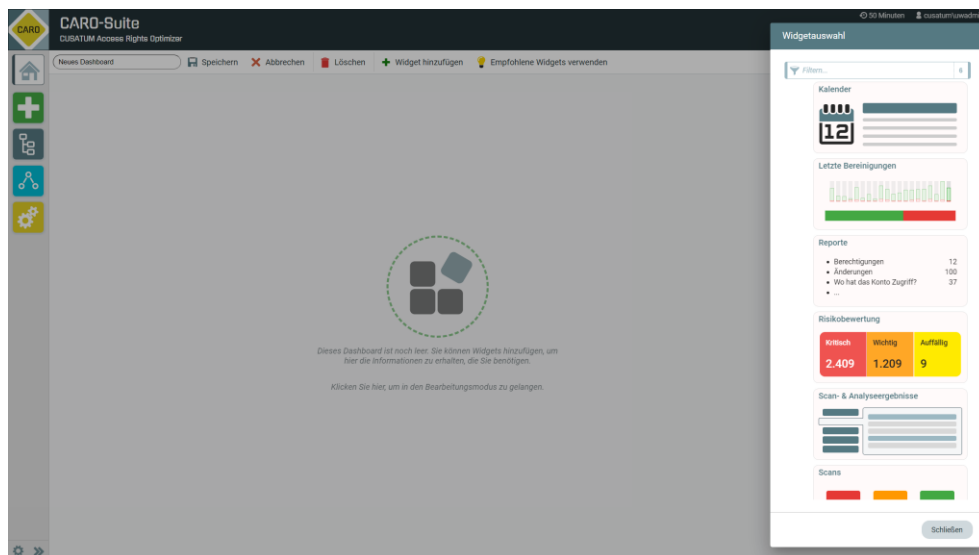
Sie können die Größe der einzelnen Widgets anpassen. Dazu in der rechten unteren Ecke mit der Maus einfach „ziehen“ und die Größe nach Ihren Wünschen verändern. In der dabei dunkel hinterlegten aktuellen Größen-Anzeige sehen Sie die aktuelle Breite und Höhe des Widgets **18 x 10**.



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.



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

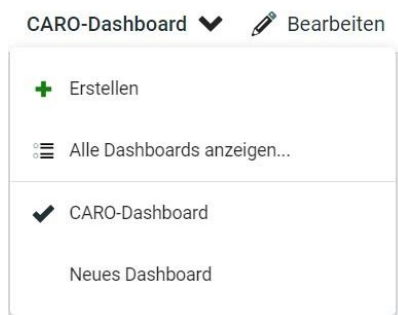


Hinweis: Sie können mehrere Widgets mit der gleichen Funktionalität hinzufügen. In einem späteren Schritt können Sie die Inhalte eines Widgets mit Filtern an Ihre Bedürfnisse anpassen.



Ein neues Dashboard erzeugen

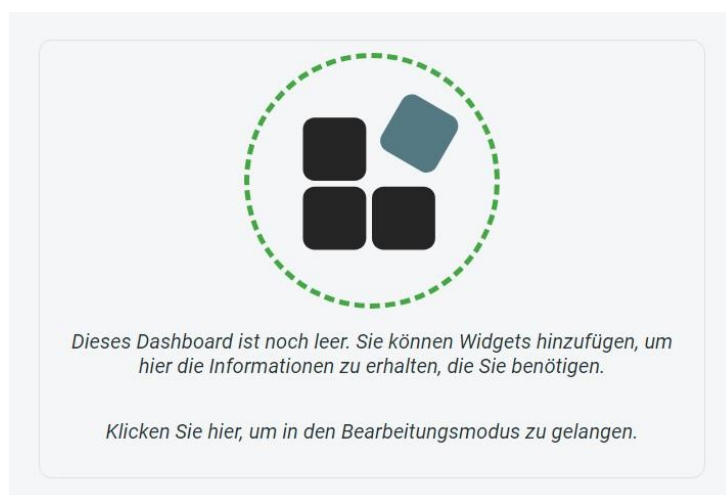
Sie können jederzeit ein neues Dashboard erstellen über das Menü **CARO-Dashboard**. Die Anzahl an Dashboards ist dabei nicht begrenzt.



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



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?
	Risikobewertung	Analyse und Risk Assessment	Analyse der Berechtigungsprobleme, sortiert nach gescanntem System, filterbar nach Zeit
	Letzte Bereinigungen	Fortschritt der Bereinigungen	Anzeige aller Bereinigungen über einen zeitlichen Verlauf von Tagen oder Wochen, Filterung nach einzelnen gescannten Systemen möglich
	Kalender	Status und Aufgabenplanung	Anzeige aller Scans im Journalmodus, Wann findet der nächste geplante Scan statt, Filterung nach Scans, Änderungen oder Reporten möglich
	Scans	Status der Scans	Anzeige der Scans gefiltert nach deren Status, erfolgreich ausgeführt, mit Warnungen oder mit Fehlern
	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.

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 Systems, wo im gewählten Zeitbereich Berechtigungsprobleme gefunden wurden.



Detailansicht

Risikobewertung - 7 Tage Rückblick

Übersicht

Name	Kritisch	Wichtig	Auffällig
CUSATUM	342	156	6.837
fileserver	6	1	0

Nach Auswahl eines Systems in der Tabelle öffnet sich die Liste aller dazugehörigen Analysen:

Risikobewertung - 7 Tage Rückblick

Übersicht

CUSATUM

Analysen

Name	Status	Ergebnis	Datum
cusatum.de	✓	2.445	18.24
cusatum.de	✓	2.445	Do., 04.04.
cusatum.de	✓	2.445	Mi., 03.04.

cusatum.de

Account Risk- & Compliance-Assessment

Ausführung Risikobewertung Änderungen (0) Reporte (0)

Erkannte Risiken

Kritisch	Wichtig	Auffällig
114	52	2.279

Probleme bewerten

Alle Risiken (6 Analysen) ☒ Alles auswählen ☐ Alles abwählen

Problem	Anzahl
Benutzer-Kennwort läuft nicht ab	104
Inaktive Computer	10
Inaktive Benutzer	52
Benutzer mit veraltetem Kennwort	2.014
Leere Gruppen	173
Gruppen ohne Beschreibung	92

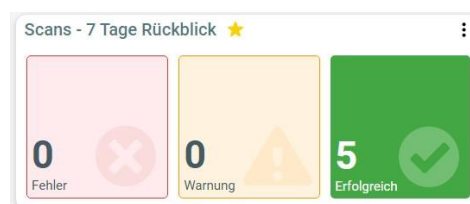
Nach Größe sortieren

- 104
- 10
- 52
- 2.014
- 173
- 92

Bewerten

Widget Scans

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





Detailansicht

The screenshot displays the 'Detailansicht' (Detail View) of scan results. At the top, there's a summary bar with 'Scans - 7 Tage Rückblick' and a 'Favoriten' (Favorites) icon. Below this, a status bar shows counts: 5 Alle (All), 0 Fehler (Errors), 0 Warnung (Warnings), and 5 Erfolgreich (Successful). A 'Filtern...' (Filter) button is also present. The main content area is divided into two panels. The left panel, titled 'Scans', lists several scan entries for 'cusatum.de' and 'Abteilungen (fileserver)', each with a status icon and a date. The right panel, titled 'Ausführung' (Execution), shows the details of a specific scan. It includes a 'Erneut ausführen' (Run again) button, a 'Löschen' (Delete) button, and a 'Fehlerdetails ein- oder ausblenden' (Toggle error details) button. The execution details show a successful completion on Friday, 5.4.2024, at 18:24, taking 1 minute and 5 seconds. It lists four steps: 'Ressourcen erfassen' (Enumerate resources), 'Konten analysieren' (Analyze accounts), 'Unbekannte Konten analysieren' (Analyze unknown accounts), and 'Konten analysieren' (Analyze accounts). Each step has a green checkmark and a brief description of the action performed.

Über die Leiste der Scan-Kategorien im oberen Bereich können Sie die Scan-Ausführungsstatus filtern. Sie können Scans neu ausführen, umplanen (für geplante Scans) oder löschen. Für Analysen, bei denen bereits eine Bewertung durchgeführt wurde, können Sie über [Letzte Bewertung fortsetzen](#) zum Risikobewertungs-Widget navigieren und damit an Ihre letzte Bewertung anknüpfen.

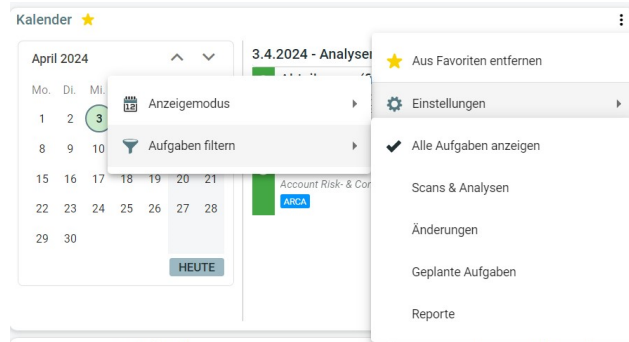
Widget Kalender

The screenshot shows the 'Widget Kalender' (Calendar Widget). It features a calendar view for March 2024, with dates from Monday to Sunday. The 16th of March is highlighted as 'HEUTE' (Today). To the right of the calendar, there's a list titled '16.3.2024 - Analysen, Änderungen und Reporte' (16.3.2024 - Analyses, Changes and Reports). This list contains four entries, each with a green checkmark and a task name: 'Tests Erlaubte Besitzer sicherstellen' (16.03., 14:10), 'Testshare_MARS (fileserver) Erforderliche Kontozugriffsrechte analysieren' (16.03., 08:00), 'Tests Erlaubte Besitzer sicherstellen' (16.03., 05:00), and 'Tests Erlaubte Besitzer sicherstellen' (16.03., 02:30). Each entry also has a small icon representing the task type.

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:

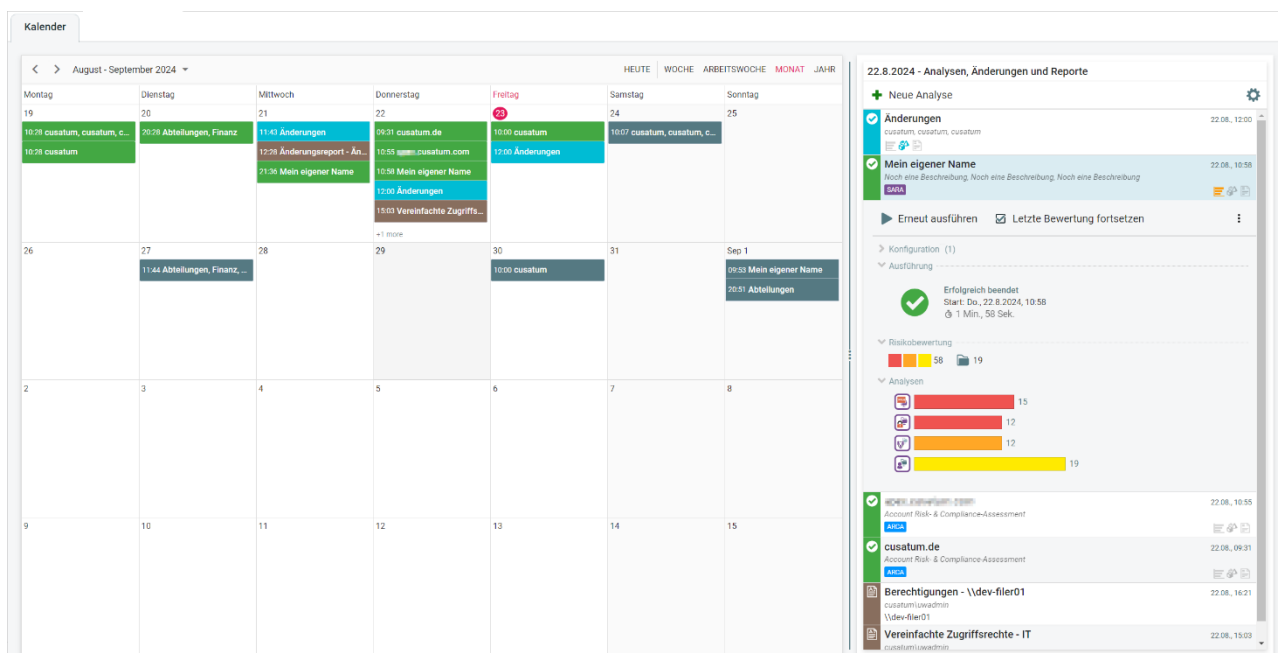
- Heute
- Kalender und Liste
- Kalender.

Oder Sie setzen den Anzeigefilter für Ihre Aufgaben:

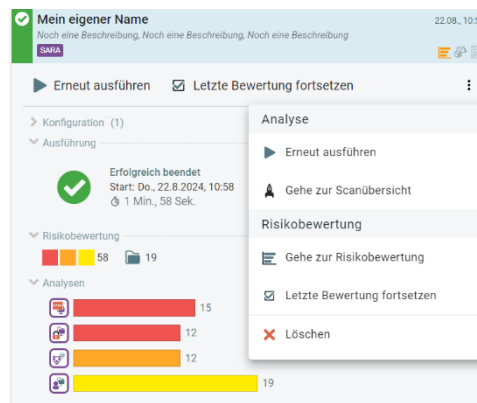


Detailansicht

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 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.

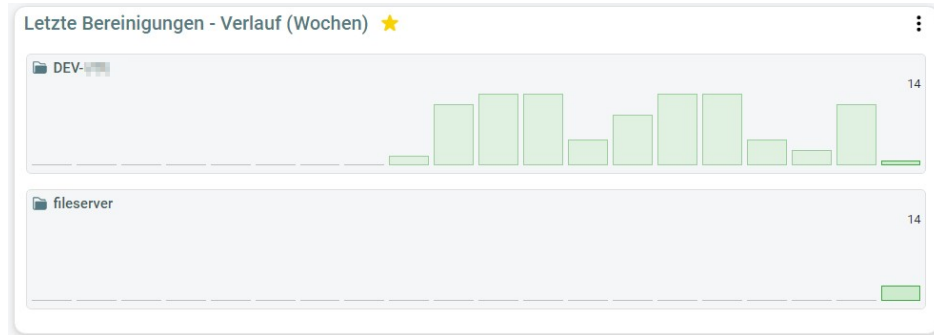




Widget letzte Bereinigungen

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.

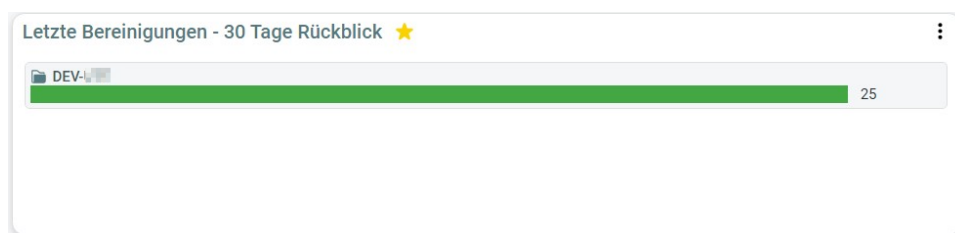


Wurden für Bereinigungen einzelne Änderungen nicht ausgeführt, wird CARO diese Rot markieren:



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



Neue Bereinigung: In 5 Schritten Ihr System bereinigen

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.



LARS

Best Practice-Tipp: Falls Sie eine Listgruppenanalyse mit dem Baustein 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 nutzen. CARO bietet dazu verschiedene Analysen für die Technologien Active Directory und Entra ID an. Nach der Auswahl Ihres Einstiegspunktes erhalten Sie eine gefilterte Ansicht der pro Technologie vorhandenen Risiko-Analysen:

Analysen für Active Directory

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

Risiko-Analysen (8/8)

☒ Deaktivierte Benutzer mit x Tagen inaktiv
Active Directory - Deaktivierte Benutzer, die mindestens x Tage nicht angemeldet waren.

☒ 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.

☒ Deaktivierte Benutzer
Active Directory - Analysiere alle Benutzer, die deaktiviert sind.

☒ Inaktive Benutzer
Active Directory - Analysiere alle Benutzer, ob sie zu lange nicht angemeldet waren.

☒ Benutzer-Kennwort läuft nicht ab
Analysiere alle Benutzer mit nie ablaufenden Kennwörtern

☒ Benutzer mit veraltetem Kennwort
Active Directory - Analysiere alle Benutzer, ob sie zu lange nicht ihr Kennwort verändert haben.

Analysen für Entra ID

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

Risiko-Analysen (9/9)

☒ Best Practices: Cloud-native-Konten Rollenzuweisungen
Entra ID - Best Practices für die ausschließliche Nutzung von Cloud-native-Konten für Rollenzuweisungen.

☒ Best Practices: Globale Admin-Rolle
Entra ID - Best Practices für die Globale Administrator Entra-Rolle.

☒ Best Practices: Gruppen Rollenzuweisungen
Entra ID - Best Practices für die ausschließliche Nutzung von Gruppen für Rollenzuweisungen.

☒ Best Practices: Privilegierte Rollen
Entra ID - Best Practices für privilegierte Entra-Rollen.

☒ Ablaufende Clientschlüssel
Entra ID - Analysiere alle Anwendungs-Registrierungen nach ablaufenden Clientschlüsseln.

☒ Globale Administratoren
Entra ID - Analysiere alle Globalen Administratoren.

☒ Inaktive Gast-Benutzer
Entra ID - Analysiere alle Gast-Benutzer, ob sie zu lange nicht angemeldet waren.

☒ Reine Online-Benutzer
Entra ID - Analysiere alle Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.

☒ Inaktive Reine Online-Benutzer
Entra ID - Analysiere alle inaktiven Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.



Für einige Analysen können Sie zusätzliche Einstellungen für Ihren Scan und den späteren 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 Passwort-Alter in Tagen
1 - 9.999

In der Bewerten-Ansicht sehen Sie dann zusätzliche Details zu den ARCA-Analysen:

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 Bereinigung auch automatisch durchführen lassen. Dadurch werden Ihre Prozesse automatisiert, eine manuelle Überprüfung ist nicht notwendig.

Automatische Bereinigung
Die automatische Bereinigung umfasst die Schritte Bewerten und Bereinigen

☒ Bereinigung automatisch durchführen

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

Risikobewertung und Analyse

Risikobewertung

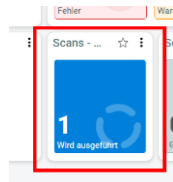
Nach dem Start des Scans können Sie zum Home-Screen der CARO-Suite zurückkehren. Sie sehen hier das Dashboard der CARO-Suite.

The screenshot shows the CARO-Suite dashboard with the following sections:

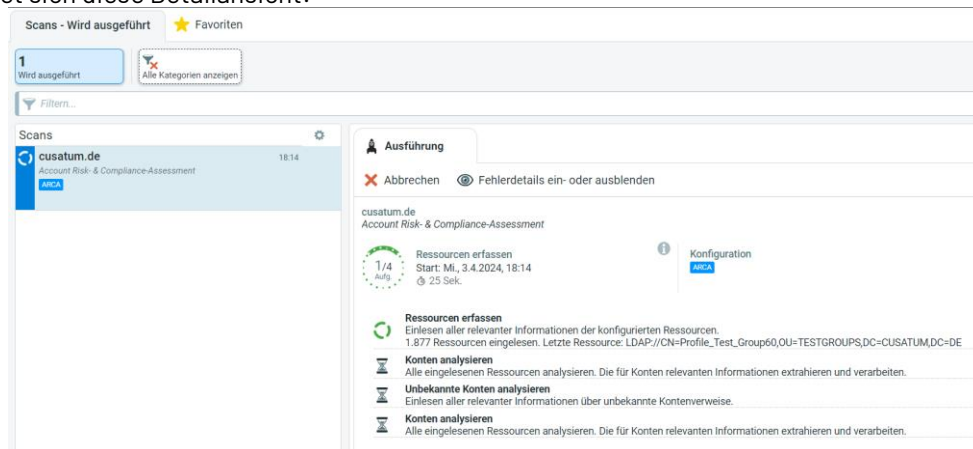
- Risikobewertung - 7 Tage Rückblick:** Three colored boxes (Kritisch, Wichtig, Auffällig) each showing a count of 0.
- Letzte Bereinigungen - Verlauf (Wochen):** A section indicating no data is available.
- Letzte Bereinigungen - 30 Tage Rückblick:** Another section indicating no data is available.
- Kalender:** A calendar view for April 2024.
- 3.4.2024 - Analysen, Änderungen und Berichte:** A summary card for the current date.
- Scans - 7 Tage Rückblick:** Three colored boxes (Fehler, Warnung, Erfolgreich) showing counts of 0.
- Scans & Analyseergebnisse:** A section showing the current scan status (Heute (1)).
- Scans - 1 Tag:** A card showing 1 scan.
- Scans - 0 Tag:** A card showing 0 scans.
- Reporte:** A section indicating no data is available.



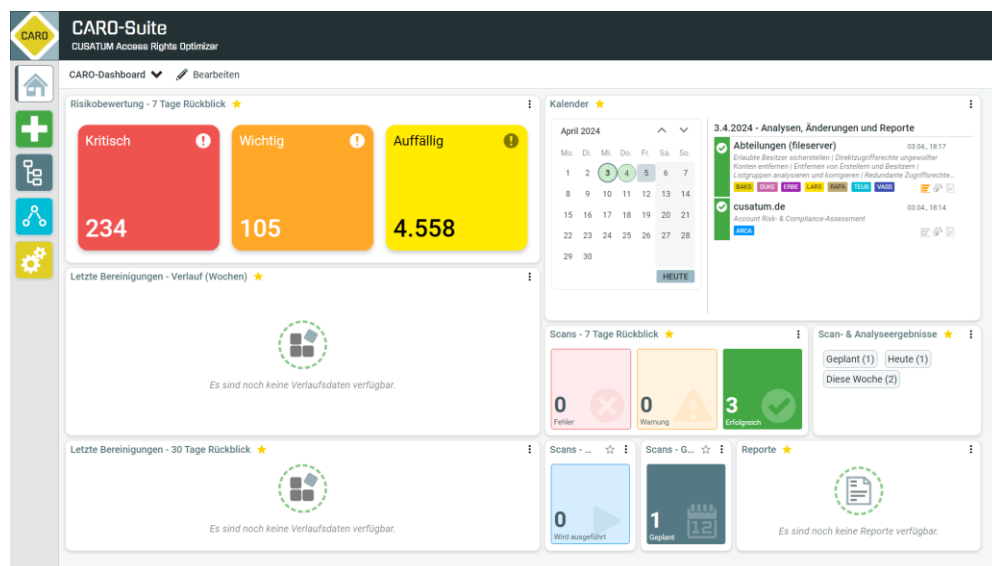
Das Dashboard ist dabei in Widgets aufgeteilt, wobei im linken Bereich die Risikobewertung und Bereinigungen im Fokus stehen. Auf der rechten Seite sind die Status-Informationen der Scans und Aufgaben zu finden. Sie können sich eigene Dashboards konfigurieren, um den Fokus auf Ihre jeweiligen Aufgaben 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:



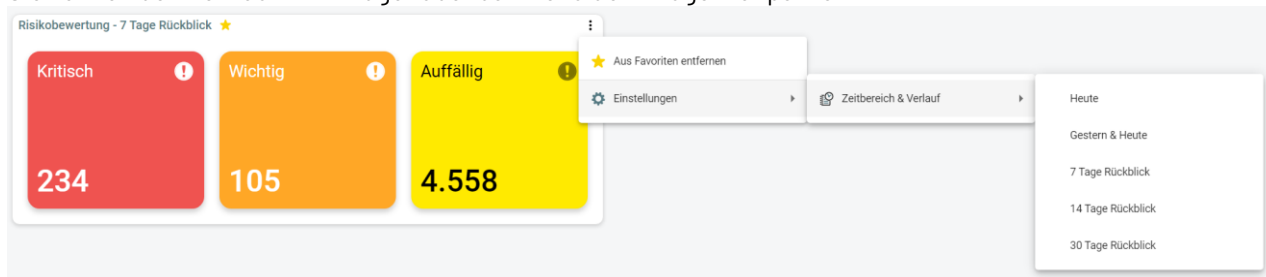
Nach Fertigstellung Ihrer ersten Scans für Filesystem und Active Directory finden Sie im Dashboard automatisch Ihre ersten Risikobewertungen auf der linken Seite im Widget [Risikobewertung](#).



Die Risiko-Bewertung ist sortiert nach den gescannten Systemen und ist sortiert nach den 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**.



Hinweis: Die Einstufungen der einzelnen Analysen in die Kategorien *kritisch*, *wichtig* oder *auffällig* können Sie in Ihrem CARO-System anpassen. Wenden Sie sich dazu unseren Support support@cusatum.de

Risikobewertung	Bereinigungsbausteine	Erklärung	Analysen
kritisch	<div> <div>VASS</div> <div>ARCA</div> <div>RAPA</div> <div>DUKE</div> <div>DARS</div> <div>BAKS</div> <div>SARA</div> </div>	<p>Diese Analysen finden Berechtigungsfehler, die von unseren Experten als kritisch eingestuft werden.</p> <p>Kritische Fehler entstehen durch unzulässige Zugriffsrechte und sollten vorrangig bereinigt werden.</p>	<ul style="list-style-type: none"> ✓ Erlaubte Besitzer-Analyse ✓ Direkte Benutzer-Berechtigungen ✓ Redundante Zugriffsrechte ✓ Unterbrochene Vererbung ✓ Inaktive Computer ✓ Kennwort läuft nie ab ✓ Aktivierte Vererbung in Freigaben ✓ Offene Freigaben ✓ Privilegierte Rollen ✓ Globale Administrator-Rolle ✓ Anzahl Globaler Admins ✓ Ablaufende Clientschlüssel



wichtig		<p>Diese Analysen finden weitere als wichtig eingestufte Probleme in Ihrem System.</p> <p>Solche relevanten Probleme sollten zeitnah behoben werden.</p>	<ul style="list-style-type: none"> ✓ Ersteller-Besitzer ✓ Mindest-Berechtigungen ✓ Verschobene Verzeichnisse ✓ Ungewollte Konten ✓ Inaktive Benutzer ✓ Listgruppenanalyse ✓ Jeder-Vollzugriff Freigaben ✓ Gruppen-Rollenzuweisungen ✓ Cloud-Native Konten Rollenzuweisungen ✓ Inaktive Gastbenutzer
auffällig		<p>Es werden Sicherheitsauffälligkeiten in den Zugriffsrechten gefunden.</p> <p>Diese Auffälligkeiten sollten nach unserer Erfahrung durch Ihre Administratoren überprüft werden.</p>	<ul style="list-style-type: none"> ✓ Verwaiste Kontoreferenzen ✓ Veraltetes Kennwort ✓ Deaktivierter Benutzer ✓ Leere Gruppen ✓ Gruppen ohne Beschreibung ✓ Nicht-administrative Freigaben ✓ Inaktive Cloud-Native Benutzer ✓ Cloud-Native Benutzer

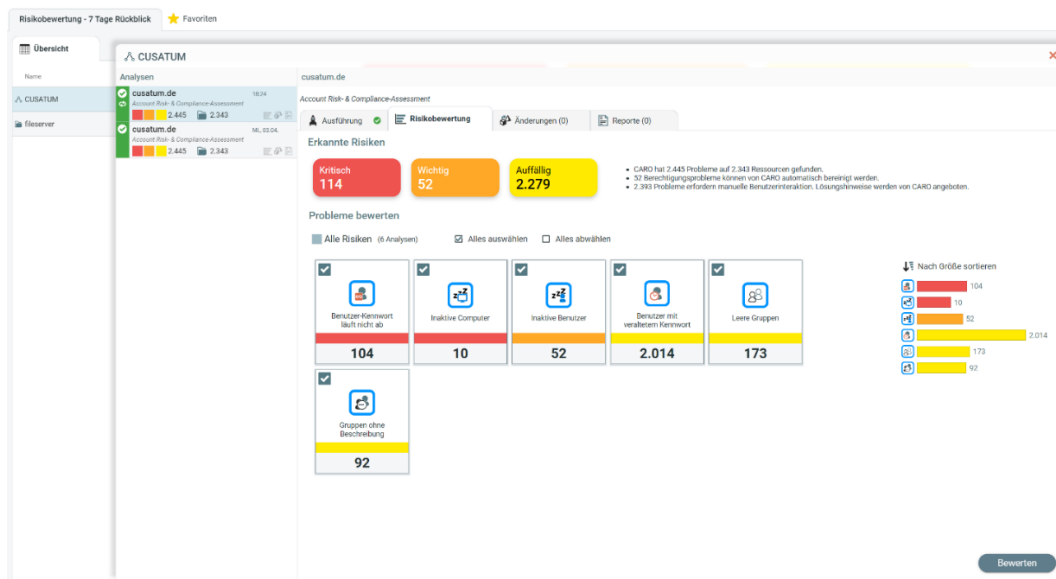
Auswahl der Systeme

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.

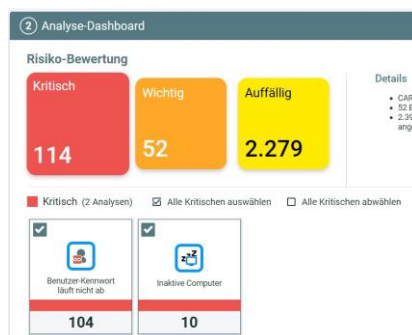


Hintergrund: CARO speichert Detail-Informationen zu den Analysen maximal 10 Tage (Standardeinstellung). Die Risikobewertungen mit den Statistiken hingegen werden dauerhaft in der Datenbank hinterlegt.

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“).





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.

4 Bereinigen der Berechtigungsprobleme

Probleme 347 Seiten 1 / 1 13 Pfade wurden zum Bereinigen ausgewählt

Ressource	Änderungen	Aktionen
\\fileserv\\Testshare_Prototype2	+	2
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\HR\\extern	-	1
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\HR\\extern\\Anweisungen\\Arbeitsanweisung\\Arbeitsbereich 4	-	38
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\HR\\extern\\Anweisungen\\Offizielles Wording	-	38
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\HR\\extern\\Anweisungen\\Sicherheitsanweisung	-	38
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\IT\\Linux	-	38
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\IT\\Linux\\Standardssoftware	-	1
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\IT\\OS\\Systemprogramme	-	38
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\IT\\Windows	-	1
\\fileserv\\Testshare_Prototype2\\Abteilungslage\\IT\\Windows\\Drittanbieter Software	-	38
\\fileserv\\Testshare_Prototype2\\Automatismus\\AI\\Algorithmen\\Geheime Projekte\\V.I.K.I	-	38
\\fileserv\\Testshare_Prototype2\\Automatismus\\AI\\Algorithmen\\Logik	-	38
\\fileserv\\Testshare_Prototype2\\Automatismus\\AI\\Deep learning\\Versuche	-	38

2 Aktionen

- Berechtigungen hinzufügen (1 Aktion)
 - CUSATUM\\TestUserMars
- Besitzer ändern (1 Aktion)
 - Administratoren → Domänen-Administratoren
 - Besitzer von Unterordnern nicht ändern
 - Besitzer von Dateien nicht ändern

Zurück 347 Probleme ausgewählt Jetzt bereinigen

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

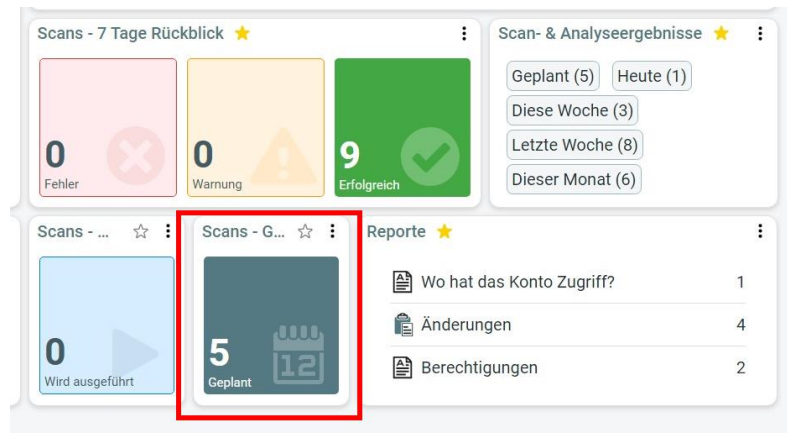
Im Tab **Änderungen** sehen Sie alle durchgeführten Änderungen noch einmal als Liste.

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.

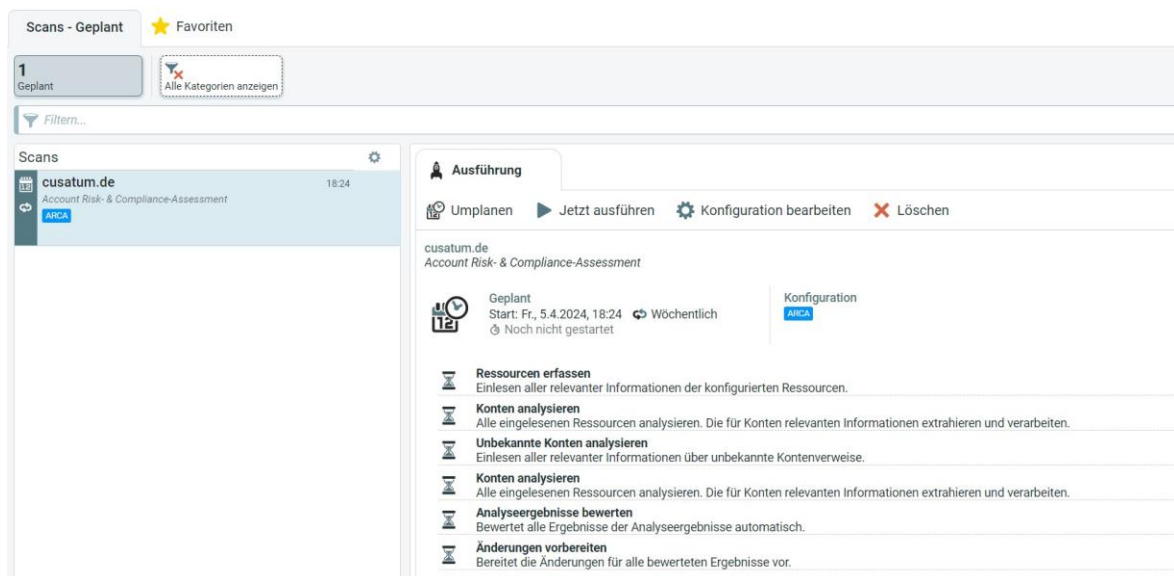


Scan und Analysen wiederkehrend planen

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:

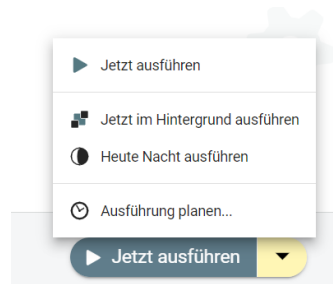


Sie können diesen Scan umplanen oder sofort neu starten. Sie können sich hier auch alle Scans anzeigen lassen, indem Sie den Filter temporär zurücksetzen:



Scans wiederkehrend planen

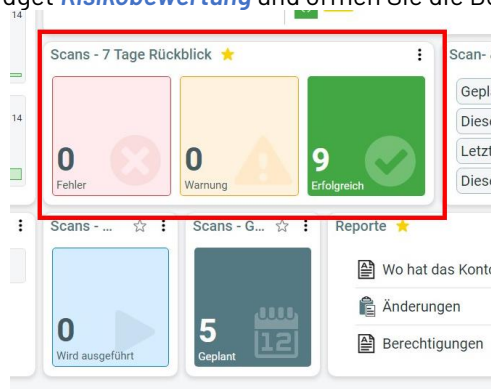
Vor dem Ausführen eines Scans können Sie wählen, ob Sie den Scan sofort ausführen möchten. Eine genaue Zeitplanung ist ebenfalls möglich über den Menüeintrag [Ausführung planen...](#)



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

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 als erstes angezeigt. Eine Suchfunktion zum schnellen Auffinden Ihrer bestehenden Analysen, Änderungen oder Reporte hilft Ihnen zusätzlich.



The screenshot displays the 'Scan- & Analyseergebnisse' section. On the left, a list of analyses is shown, categorized by 'Geplant (1)', 'Heute (1)', and 'Diese Woche (3)'. Each entry includes the start time, duration, name (e.g., 'cusatum.de', 'Abteilungen (fileserv)'), and a risk assessment (e.g., '2.445', '2.343'). A '1 Bewertung' button is visible for each entry. On the right, a detailed view of a scan is shown, indicating it was 'Erfolgreich beendet' (Successfully completed) with a start time of 'Fr., 5.4.2024, 14:30' and a duration of '9 Sek.'. A 'Konfiguration' button is also present.

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

This block shows a detailed view of a scan entry. It includes the start time 'Do., 4.4.2024, 18:24', duration '1 Min.', and name 'cusatum.de'. Below this, there are two colored squares (red and yellow) followed by the values '2.445' and '2.343'. At the bottom, there is a '1 Bewertung' button with a checkmark icon.

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.

The screenshot shows the 'Weitere Elemente (1)' section. It contains a box titled 'Elemente aus gelöschten Analysen'. Inside this box, there are two buttons: '1 Änderung' (with a green icon) and '1 Report' (with a red icon).

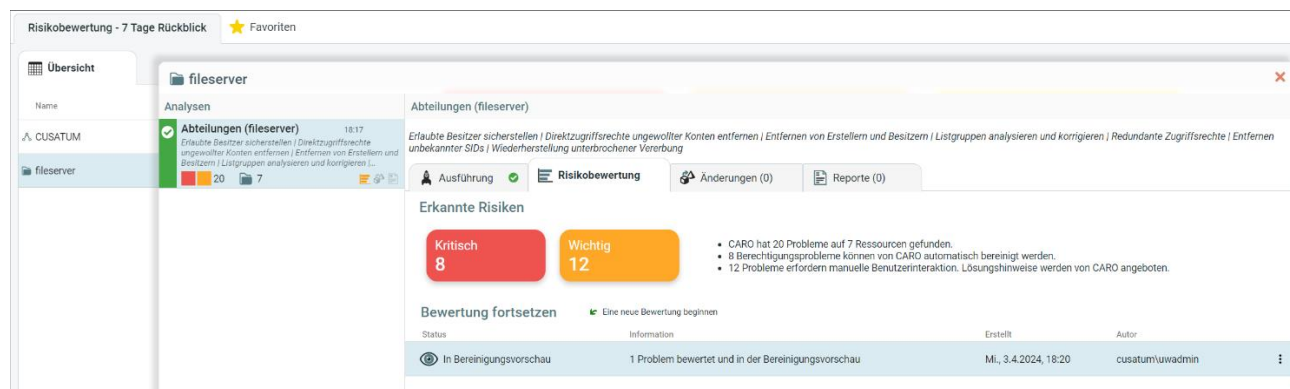


Weiter Aufräumen nach einer durchgeführten Analyse

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**.

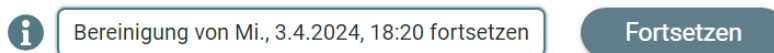


Sie können Ihre Bewertung fortsetzen, eine neue Bewertung starten, vorherigen Änderungen ansehen oder einen Report über durchgeführte Änderungen erstellen, welche CARO durchgeführt hat.



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 Reporte-Widget einsehbar. Die CARO-Suite sortiert die verschiedenen Report-Typen in die Tab-Ansichten ein: Berechtigungs-Reporte, Berechtigungs-Differenz-Reporte, Wo hat ein Benutzer-Zugriff-Report oder Änderungsreporte.



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



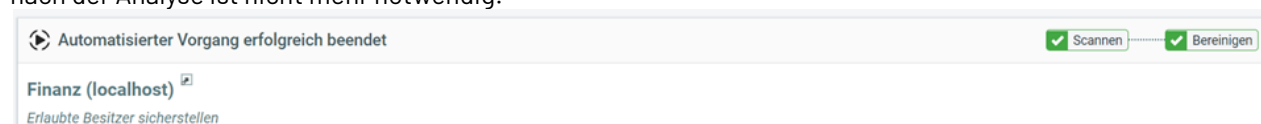
Reporte ★		
📄	Wo hat das Konto Zugriff?	1
📄	Änderungen	4
📄	Berechtigungen	2



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

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.



Automatische Bereinigung
Die automatische Bereinigung umfasst die Schritte Bewerten und Bereinigen

☒ **Bereinigung automatisch durchführen**

Bewertungsregeln (1/9) ☒ ☐

☒ **Bereinige alles**
Alle gefundenen Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 1.000**
Bis zu 1.000 gefundene Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 5.000**
Bis zu 5.000 gefundene Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 10.000**
Bis zu 10.000 gefundene Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 20.000**
Bis zu 20.000 gefundene Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 50.000**
Bis zu 50.000 gefundene Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 100.000**
Bis zu 100.000 gefundene Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 200.000**
Bis zu 200.000 gefundene Probleme werden automatisch bewertet und bereinigt

☐ **Bereinige 500.000**
Bis zu 500.000 gefundene Probleme werden automatisch bewertet und bereinigt

Kommentar

☒ **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.

☐ **Speicherbedarf minimieren und auf Details verzichten**
Die Anzeige der vorgenommenen Änderungen beschränkt sich auf die Statistik und verbraucht dadurch deutlich weniger Datenbankspeicher.



Hinweis: Falls Sie hier andere Bewertungsregeln benötigen bzw. eigene angepasste Bewertungsregeln benutzen möchten, dann wenden Sie sich bitte an unseren Support support@cusaturn.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
CUSATUM	228	104	4.558
fileserv	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		
✓	cusatum.de	Do., 04.04.
	Account Risk- & Compliance-Assessment	
	2.445	2.343
✓	cusatum.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.

Risikobewertung - 7 Tage Rückblick

Favoriten

Übersicht

Name

CUSATUM

fileserv

fileserv

Analysen

Abteilungen (fileserv)

18.17

✓

20

7

Abteilungen (fileserv)

Erlaubte Besitzer sicherstellen | Direktzugriffsrechte ungewollter Konten entfernen | Entfernen von Erstellern und Besitzern | Listgruppen analysieren und korrigieren | Redundante Zugriffsrechte | Entfernen unbekannter SIDs | Wiederherstellung unterbrochener Verbindung

Ausführung

Risikobewertung

Änderungen (0)

Reporte (0)

Erkannte Risiken

Kritisch

8

Wichtig

12

• CARO hat 20 Probleme auf 7 Ressourcen gefunden.

• 8 Berechtigungsprobleme können von CARO automatisch bereinigt werden.

• 12 Probleme erfordern manuelle Benutzerinteraktion. Lösungshinweise werden von CARO angeboten.

Bewertung fortsetzen

Status

Information

Erstellt

Autor

In Bewertungsvorschau

1 Problem bewertet und in der Bewertungsvorschau

Mi., 3.4.2024, 18:20

cusatum\wvadmin



4. Bereinigung fortsetzen

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



Bereinigung von Mi., 3.4.2024, 18:20 fortsetzen

Fortsetzen

Weitere Informationen zur generellen Benutzung des CARO-Dashboards finden Sie im Kapitel [Widgets und ihre Funktion](#).

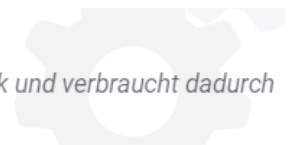
Speicherbedarf minimieren

Diese Option bewirkt, dass für die Ergebnisse der Änderungen, welche CARO vornimmt, nicht mehr die Details abgespeichert werden. Die Ergebnis-Seite mit den Einzeländerungen bleibt dann leer, ein Report mit dem Gesamtergebnis kann trotzdem erzeugt werden.



Speicherbedarf minimieren und auf Details verzichten

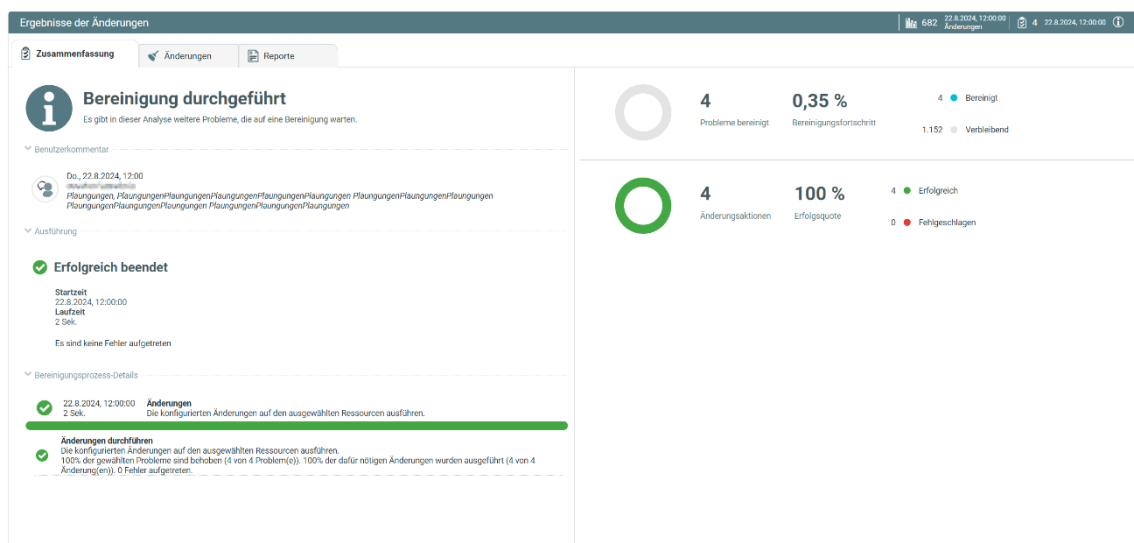
Die Anzeige der vorgenommenen Änderungen beschränkt sich auf die Statistik und verbraucht dadurch deutlich weniger Datenbankspeicher.



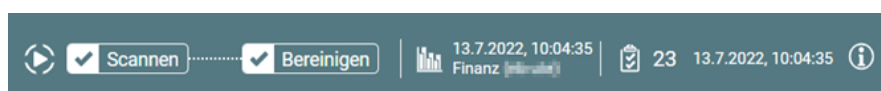
Ergebnisse

Wenn die automatische Bewertung und Bereinigung abgeschlossen sind, dann sehen Sie das Ergebnis der Bereinigung auf der Home-Seite: alle Probleme wurden beseitigt.

Auf der Ergebnis-Seite der Änderungen können Sie ebenfalls sehen, wieviel Berechtigungsfehler bereinigt wurden.



Auch die „Pipeline-Leiste“ rechts oben zeigt die Informationen kompakt an:



Sie können einen Report erstellen, um sich die Änderungen im Detail anzusehen. Auch nicht durchführbare Änderungen werden dokumentiert:



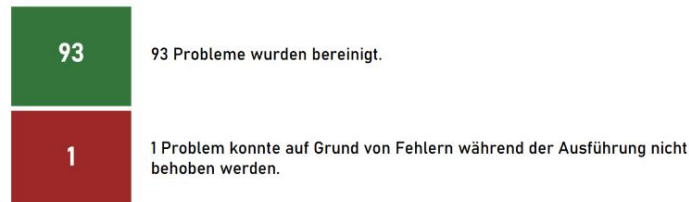
CARO Report - Modifications

Seite 1/10

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:

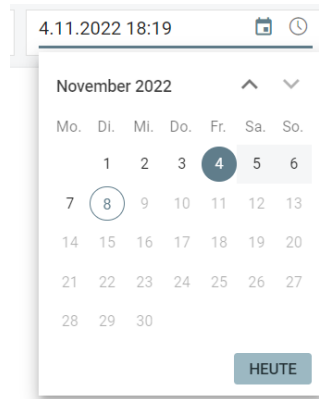
Die Ressourcen-Ansicht zeigt zu einem gewählten Datum für alle durchgeführten Scans die Berechtigungslage an. Derzeit werden AD-Strukturen und Fileserver-Strukturen (mit lokalen Konten) unterstützt. Sie können über eine Navigationsleiste durch die Ordner-Strukturen navigieren, Ordner suchen und sich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



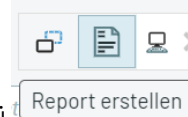


Standardmäßig werden immer die neuesten Scans pro Technologie angezeigt. Die Auswahl eines älteren Scans erfolgt über die Kalender-Datumsauswahl. Der Kalender zeigt nur den Zeitraum zwischen dem ältesten und dem neuesten Scan-Datum an. Alle Scan-Zeiten dazwischen können Sie frei auswählen. CARO wählt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



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.



5.4.2024 18:24

Abteilungen

Besitzer: fileserver\Administrators Auffälligkeiten: 2 Auffälligkeiten unterhalb: 2

✓ Berechtigungseinträge Freigabe Eigenschaften

Filtern... 4 Berechtigungsfilter

Konto				Berechtigung
Lokales System				Vollzugriff
fileserver\Administrato...	24	!		Vollzugriff
CUSATUM\abadmin				Vollzugriff
CUSATUM\Group 0	6			Lesen & Ausführen

Details CUSATUM\Group 0

Berechtigungen Mitglieder (6) Mitglied von (0)

Filtern... Alle Direkte Beziehungen Indirekte Beziehungen Mehrfache Beziehungen

Konto	LDAP-Container	Direkt	Indirekt	Ebene
CUSATUM\Andreas Angestellter	Testusers			1
CUSATUM\Caro Weg	CARO-Testing			1
CUSATUM\Michael Manager	Testusers			1
CUSATUM\Musterfrau beate	Testusers			1

Kontenansicht
Öffnet die Kontenansicht und zeigt die Gruppenmitgliedschaften des Kontos an

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

Eine IST-Berechtigungsanalyse starten

Für die Anzeige Ihrer IST-Berechtigungslage ist nur der Baustein **EBIS** notwendig. Zum Scannen der Berechtigungen gehen Sie links im CARO-Menü zu „Neue Bereinigung starten“ und wählen Sie nur den Baustein EBIS aus. Nach Auswahl Ihrer gewünschten Scan-Einstiegspunkte starten Sie den Scan mit der Analyse.

EBIS Zugriffsrechte-Rekorder
✓

Zeichnet alle Zugriffsrechte der konfigurierten Systeme auf.

1 Scan konfigurieren

① Wählen Sie Ihre Aufgaben

eb
1 / 11

EBIS Zugriffsrechte-Rekorder
✓

Zeichnet alle Zugriffsrechte der konfigurierten Systeme auf.

② Wählen Sie Ihre Scan-Einstiegspunkte

Wählen Sie Ihre Scan-Einstiegspunkte aus konfigurierten Scan-Pfaden, mit der Konfiguration der maximalen Scan-Tiefe und den Scan-Anmeldedaten.

Einstiegspunkte wählen

Es wurden noch keine Einstiegspunkte für den Scan gewählt.

③ Konfigurieren der Aufgaben

Scan-Einstellungen
Einstellungen für Filesystem-Einstiegspunkte

☐ Konfigurierte Einstellungen für alle ausgewählten Filesystem-Einstiegspunkte überschreiben

4 Maximale Scantiefe
1 - 99


2 Begrenzung der vollständigen Speicherung
1 - 99



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:

The screenshot displays the CARO-Suite WebClient interface. At the top, there is a 'Kalender' (Calendar) widget for April 2024, with the 5th highlighted. To its right is a '5.4.2024 - Analysen, Änderungen und Reporte' (5.4.2024 - Analyses, Changes and Reports) section. This section contains a list of scans, with one entry 'Abteilungen (fileserv) Zugriffsrechte-Rekorder' (Departments (fileserv) Access rights recorder) highlighted with a red box. This entry shows a green checkmark and the EBIS logo. Below the calendar and reports, there is a 'Scans - 7 Tage Rückblick' (Scans - 7 Day Overview) widget, also highlighted with a red box. This widget shows three categories: 'Fehler' (Errors) with 0, 'Warnung' (Warning) with 0, and 'Erfolgreich' (Successful) with 4. To the right of this is a 'Scan- & Analyseergebnisse' (Scan & Analysis Results) widget showing 'Geplant (1)' (Planned 1), 'Heute (1)' (Today 1), and 'Diese Woche (3)' (This week 3). At the bottom, there are three more widgets: 'Scans - ...' showing 0 'Wird ausgeführt' (Being executed), 'Scans - G...' showing 1 'Geplant' (Planned), and 'Reporte' (Reports) showing 'Es sind noch keine Reporte verfügbar.' (No reports are available yet).

Öffnen Sie über das CARO-Menü  direkt die Ressourcen-Ansicht, um die IST-Berechtigungssituation anzuzeigen.



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

Verteilung von Berechtigungen (Statistiken)

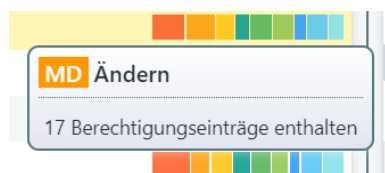
Die Verteilung der Berechtigungskategorien sehen Sie jeweils rechts als farbiges Balkendiagramm pro Verzeichnis. So haben Sie einen schnellen Überblick über Abweichungen in Ihrer Berechtigungsvergabe. Vergleichen Sie direkt die Ordnerberechtigungen einer Verzeichnisebene miteinander auf der linken Seite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

The screenshot displays the 'global share' resource view in the CARO-Suite WebClient. The left pane shows a list of resources with columns for Name, Scan Zeit, Auffälligkeiten hier, Auffälligkeiten unterhalb, Besitzer, and Verteilung der Berechtigungen. The right pane shows a detailed view of the 'global share' resource, including a table of permissions and a bar chart showing the distribution of permissions across different categories.



Ressourcen unterhalb von 'global share' filtern...

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	Auffälligkeiten
Administrator	
Berechtigungseinträge	Scan-Probleme (1)
Warnungen (1)	
Ignoriert - maximale Scantiefe überschritten.	

Informationen zu einzelnen Berechtigungseinträgen werden rechts auf der Seite angezeigt:



Bob Baumeister

Besitzer: Domänen-Administratoren | Auffälligkeiten: Keine | Auffälligkeiten unterhalb: Keine

✓ Berechtigungseinträge | Eigenschaften | Mitglied von (7)

Filtern... 26 Berechtigungsfiler

Konto				Berechtigung		Anwenden auf
Windows Authorization Ac...	3			Spezial		
RAS and IAS Servers				Spezial	4	
CUSATUM\Exchange Trust...	1			Spezial	18	
CUSATUM\Exchange Wind...	2			Spezial	23	
VORDEFINIERT\Pre-Windo...	1			Spezial	14	
CUSATUM\Delegated Setup				Spezial		
CUSATUM\Exchange Serv...	2			Spezial	21	
CUSATUM\Organization M...	5			Spezial	14	
Ersteller Besitzer				Spezial		

Details CUSATUM\Exchange Servers

Berechtigungen | Mitglieder (2) | Mitglied von (2)

Filtern... 2

☒ Alle ☐ Direkte Mitglieder ☐ Mehrfach berechnete Mitglieder

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

Elemente pro Seite: 100 | 1 – 2 von 2 | < > | Gehe zu Seite: 1

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.

Administratoren

✓ Berechtigungseinträge

Filtern...

Konto	
Administratoren	1
Mary Dole	

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

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

Anzeige der Gruppenmitglieder

Für Gruppen werden die Mitgliedschaften aufgelöst und auf direkte oder indirekte Berechtigung analysiert:

Aron Aal
Direktes Mitglied von 'Hygienegruppe'

FK Test
Indirektes Mitglied über andere Gruppenmitgliedschaften.



Falls Mitglieder direkt und indirekt in einer Gruppe enthalten sind, wird dies ebenfalls pro Benutzerkonto in der Detailansicht angezeigt:

	Administrator	Users		(2x)
--	---------------	-------	--	------

Filter für schnelles Auffinden von Mehrfach-Berechtigungen

In der Anzeige der *Mitglieder* oder *Mitglied von* können Sie nun filtern, ob Sie nur die direkten oder nur die mehrfach berechtigten Relationen sehen wollen.

Administrator

Besitzer

Domänen-Administratoren

Auffälligkeiten

Auffälligkeiten unterhalb

Keine

Berechtigungseinträge

Eigenschaften

Mitglied von (16)

Filtern...

16

Alle

Direkte Mitglieder

Mehrfach berechnete Mitglieder

Konto

LDAP-Container

Direkt

Indirekt

Ebene

Administratoren

Builtin

(2x)

2

Administratoren

(1x)

2

Users

(1x)

2

Enterprise-Administratoren

Users

1

Domain Users

Users

1

Denied RODC Password Replication Group

Users

(4x)

2

Hygienegruppe

Users

(1x)

2

Group Policy Creator Owners

Users

1

Gruppe 3

Testgroups

(1x)

2

Remote Desktop Users

Builtin

(1x)

2

Users

Builtin

(1x)

2

Schema Admins

Users

1

L_CompanyShare_Folder A_mx

fileservers

(1x)

2

Il_Testshare_bb_Geda_list

fileservers

(1x)

3

L_Testshare_bb_Geda_IT_PDF Scan_mx

fileservers

(1x)

2

Domain Admins

Users

1

Filtern...				
<input type="radio"/> Alle <input type="radio"/> Direkte Mitglieder <input checked="" type="radio"/> Mehrfach berechnete Mitglieder				
Konto	LDAP-Container	Direkt	Indirekt	Ebene
Administratoren	Builtin		(2x)	2
Denied RODC Password Replication Group	Users		(4x)	2



Hinweis: Wenn Sie keinen Domänen-Scan durchgeführt haben, werden in der Detailansicht Gruppen nicht aufgelöst, bzw. es werden keine Mitglieder der Gruppen angezeigt.



Hinweis: Ein Ausblenden von Mitgliedern von bestimmten Gruppen als Blacklist-Konfiguration ist derzeit noch nicht möglich. Für Gruppen mit einer großen Anzahl an Mitgliedern werden diese seitenweise vom Server abgeholt. Standardmäßig werden 100 Einträge pro Seite angezeigt.

Elemente pro Seite: 100 1 – 2 von 2 < > >> Gehe zu Seite: 1

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.



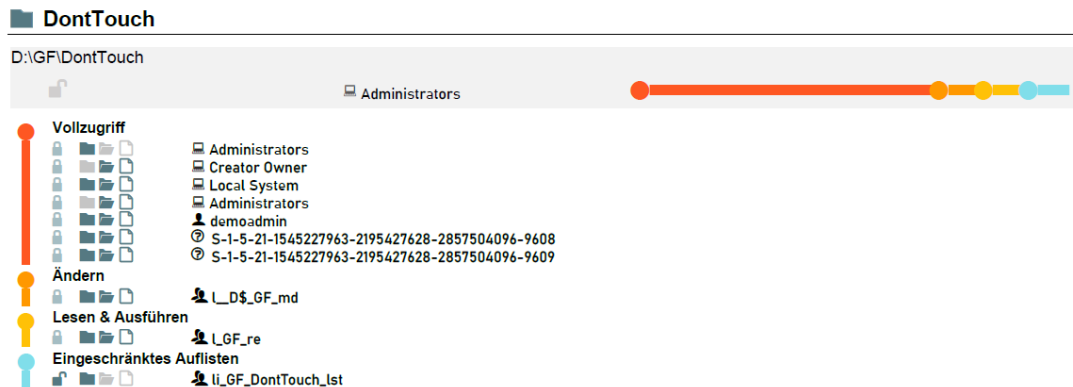


Report über die IST-Berechtigungssituation

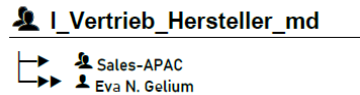
Für diesen Report werden folgende Standardparameter genutzt:

- 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:



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:

DontTouch

D:\GF\DontTouch

Administrators

Veränderungen zu GF (D:\GF)

- Vollzugriff**
 - + S-1-5-21-1545227963-2195427628-2857504096-9608
 - + S-1-5-21-1545227963-2195427628-2857504096-9609
- Eingeschränktes Ändern**
 - S-1-5-21-1545227963-2195427628-2857504096-9608
- Eingeschränktes Auflisten**
 - + li_GF_DontTouch_List

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:

Das Konto

Button zur Reporterstellung

Details Administratoren

Berechtigungen Mitglieder (2) Mitglied von (0)

drived

Das Verzeichnis

Besitzer S-1-5-21-4262257557-526714673-2123679...

Auffälligkeiten Keine

Auffälligkeiten unterhalb

Berechtigungseinträge 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...)

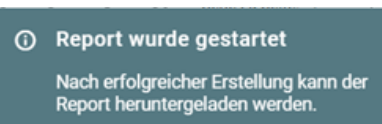
Erstellen Schließen



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 Reports, auch Ihre Änderungsreports von Bereinigungsprozessen, 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

Data Owner-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 \\fileserv\Abteilungen\IT\30_TestDaten		✓		
Berichte \\fileserv\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.

Konten-Ansicht mit Suchfunktion

Die neue Accounts-View gibt Ihnen einen klaren Überblick über Benutzer-, Gruppen- und Computerkonten. Entdecken Sie Auffälligkeiten in der Berechtigungsstruktur des Active Directory oder suchen Sie nach auffälligen Konten.

Die neue Accounts-View bietet Ihnen:

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

Durch das Active Directory navigieren

Die neue Kontenansicht wird in 3 Bereiche unterteilt: Suchergebnisse, Selektion und Gruppenmitgliedschaftsbeziehungen:



The screenshot displays the 'Suche' (Search) section of the CARO-Suite WebClient. The search bar contains 'Suche in CUSATUM'. Below it, a table shows search results for 'CUSATUM/Domänen-Benutzer'. The detailed view for this account shows its properties, including 'Common-Name', 'Description', 'City-Dist-Name', 'Group-Type', 'Object-Sid', and 'SAM-Account-Name'. The 'Kontenbeziehungen' (Account Relationships) section shows a list of related accounts and their LDAP containers.

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.

The screenshot shows the 'Suche' section with a search bar containing 'test'. Below the search bar, the 'Such-Einstellungen' dialog box is open, allowing users to configure search settings. The dialog box includes a section for 'Such-Einstellungen' and a warning message: 'Definieren Sie, in welchen Eigenschaftsfeldern die Suche durchgeführt werden soll'.

In diesem Beispiel wurden 3 Eigenschaften für die Suche konfiguriert:

The screenshot shows the 'Suche' section with a search bar containing 'test'. Below the search bar, the 'Such-Einstellungen' dialog box is open, showing 3 search criteria configured: 'company', 'department', and 'description'. A warning message is displayed: 'Bitte beachten Sie, dass die Erweiterung der Suchkriterien um viele Eigenschaften die Suche verlangsamt.' (Please note that extending the search criteria with many properties slows down the search.)

In der Suchergebnis-Liste werden dann die einzelnen Eigenschaften noch einmal aufgelistet, in denen der Suchstring gefunden wurde. Dazu einfach über das Symbol

The screenshot shows the search results list with the text '30 / 1.339 Ergebnisse der aktuellen Suche'. Below the results, the 'Such-Einstellungen' dialog box is open, showing 3 search criteria configured: 'company', 'department', and 'description'. A warning message is displayed: 'Bitte beachten Sie, dass die Erweiterung der Suchkriterien um viele Eigenschaften die Suche verlangsamt.' (Please note that extending the search criteria with many properties slows down the search.)



Sie können nun die gefundenen Accounts einzeln selektieren. In der Mitte wird das jeweils selektierte Konto aktualisiert:

company: autotest gmbh		
▼	CUSATUM\ArcaTest DontCh...	7 User
company: autotest gmbh		
▼	CUSATUM\ArcaTestDeacCo...	1 Computer
Name: cusatum\arcatestdeaccomp		
▼	CUSATUM\ArcaTestEmptyGr...	Groups
description: empty group for arca autotest		
▼	CUSATUM\ArcaTestNoDescr...	2 Groups

Eine Kontext-Suche für eine bestimmte Eigenschaft starten

In der Mitte werden im unteren Bereich jeweils die Eigenschaften des selektierten Kontos angezeigt. Sie können hier eine Kontext-Suche starten. Wenn Sie z.B. alle Konten mit der Eigenschaft **Autotest GmbH** suchen wollen, dann wählen Sie die Zeile an und klicken Sie auf die Schaltfläche **Suche**.

Eigenschaften	
Export Excel	
Name	Wert
Account-Expires	1/1/1970
Common-Name	Christiana Gerling
Company	Autotest GmbH
Department	Contracts
Display-Name	Christiana G
CN=Christiana	

Eine neue Suche mit diesen Suchkriterien wird gestartet:

Suche		
autotest gmbh	30 / 93	
<input type="radio"/> enthält	<input type="radio"/> beginnt mit	<input type="radio"/> endet mit
<input checked="" type="radio"/> ist gleich		
30 / 93 Ergebnisse der aktuellen Suche		
company ist gleich autotest gmbh		
Konto		LDAP-Container
company: autotest gmbh		
▼	CUSATUM\Dietwulf Feiler	7 User
company: autotest gmbh		
▼	CUSATUM\Dietz Bernhardt	7 User
company: autotest gmbh		

Excel-Kontenreport erzeugen

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




The screenshot shows the user profile for CUSATUM\Christiana Gerling. The 'Eigenschaften' (Properties) section lists various attributes like Name, Account Expires, and Email-Addresses. The 'Kontenbeziehungen' (Account Relationships) section shows a list of accounts and their relationships, including direct and indirect memberships.

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 ein Konto direkt und indirekt in einer Gruppe Mitglied ist, dann wird diese durch CARO mit einem Warnungs-Indikator  angezeigt:

The screenshot shows the user profile for CUSATUM\Testadmin. The 'Eigenschaften' section lists attributes. The 'Kontenbeziehungen' section shows a list of accounts. A red box highlights the 'fileserver\Administrators' account, which has a warning icon (yellow triangle with an exclamation mark) next to it, indicating a direct and indirect membership in a group.



CUSATUM Service GmbH

Die CUSATUM Service GmbH mit Sitz in Berlin/Brandenburg ist ein Software- und Beratungsunternehmen mit dem Fokus auf Berechtigungsmanagement und Automatisierung von Mitarbeiterprozessen. CUSATUM entwickelt die Software CARO, den CUSATUM Access Rights Optimizer. Die CARO-Suite ist eine Lösung zur automatisierten Bereinigung von IT-Strukturen in Microsoft- und virtuellen Serverumgebungen und unterstützt Unternehmen beim Berechtigungsmanagement zur Erfüllung gängiger Sicherheits- und Compliance-Richtlinien.

Herausgeber

CUSATUM Service GmbH

Hauptsitz
Wiesenweg 16
16548 Glienicke / Nordbahn

www.cusatum.de
info@cusatum.de

Support

Telefon: +49 30 9486 340 1
Mobil: +49 175 221 11 04
support@cusatum.de



Wir haben den 8MAN als Core-Team von seinen Anfängen an 10 Jahre entwickelt und den Grundstein gelegt, dass Protected Networks so erfolgreich im deutschsprachigen Raum geworden ist. In diesen Jahren durften wir uns täglich mit dem Thema DSGVO mit Schwerpunkt Berechtigungsmanagement und Rollenkonzepte auseinandersetzen. Nun dürfen unsere Kunden von den gewonnenen Erfahrungen profitieren, indem wir die CARO-Suite entwickelt haben.

Nun können unsere Kunden von den gesammelten Erfahrungen profitieren, indem wir die CARO-Suite entwickelt haben. Mit ihr sparen Sie Zeit und Geld durch saubere Berechtigungsstrukturen mit optimierten Zugriffsrechten.

Berlin, im August 2024