8MAN

Access Rights Management. Only much Smarter.

Access Rights Management

Anwenderhandbuch

Version 9

Protected Networks

Access Rights Management: Sicherheit im Netzwerk

Wir sind im Jahr 2009 angetreten die IT Sicherheit unserer Kunden einfach und effizient zu erhöhen. Uns war klar: Professionelle IT-Sicherheit endet nicht mit der Firewall, sondern einem von innen abgesicherten Firmennetzwerk.

Im Jahr 2016 haben wir mit über 900 zufriedenen Kunden weltweit eine einzigartige Marktstellung erreicht: 8MAN Access Rights Management ist längst Standard in vielen sicherheitsgetriebenen Unternehmen und Behörden. Dies wäre ohne die enge Zusammenarbeit mit unseren Kunden, Partnern und Distributoren nicht möglich gewesen.

Deshalb bedanke wir uns recht herzlich bei Ihnen und wünschen viel Spaß mit diesem Handbuch. Es umfasst das gesamte Leistungsspektrum von 8MAN und zeigt, wie Sie Ihr Firmennetzwerk von innen sichern und effizient verwalten.

Berlin im Juli 2018

Herausgeber

Protected Networks GmbH

Alt-Moabit 73
10555 Berlin

+49 30 390 63 45 - 0
Protected-Networks.com
8MAN.com

Support

+49 30 390 63 45 – 99
helpdesk@8man.com
Knowledge Base

Knowledge Management

Fabian Fischer / Jörg Brandt

T: +49 30 390 63 45-41
T: +49 30 390 63 45-81

Sie haben Feedback?

Stephan Brack

CEO Protected Networks

Matthias Schulte-Huxel

CSO Protected Networks

Haftungsausschluss

Die in diesem Dokument gemachten Angaben können sich jederzeit ohne vorherige Ankündigung ändern und gelten als nicht rechtsverbindlich.

Die beschriebene Software 8MAN wird von Protected Networks im Rahmen einer Nutzungsvereinbarung zur Verfügung gestellt und darf nur in Übereinstimmung mit dieser Vereinbarung eingesetzt werden.

Dieses Dokument darf ohne die vorherige schriftliche Erlaubnis von Protected Networks weder ganz noch teilweise in irgendeiner Form reproduziert, übermittelt oder übersetzt werden, sei es elektronisch, mechanisch, manuell oder optisch.

Dieses Dokument ist in einer Einheit zu denen auf der Website von Protected Networks veröffentlichten rechtlichen Hinweisen AGB, EULA und der Datenschutzerklärung zu sehen.

Protected Networks GmbH
Alt-Moabit 73
10555 Berlin

Berlin im Juli 2018

Inhalt

1. Warum Access Rights Management?

1.1 Zum Schutz von Daten, Informationen und Wissen

Die Firewall schützt vor externen Gefahren. 8MAN Access Rights Management schützt Daten, Information und Wissen innerhalb des Netzwerkes.

Access Rights Management beantwortet drei zentrale Fragen:

Personenebene

Wer hat wo Zugriff?

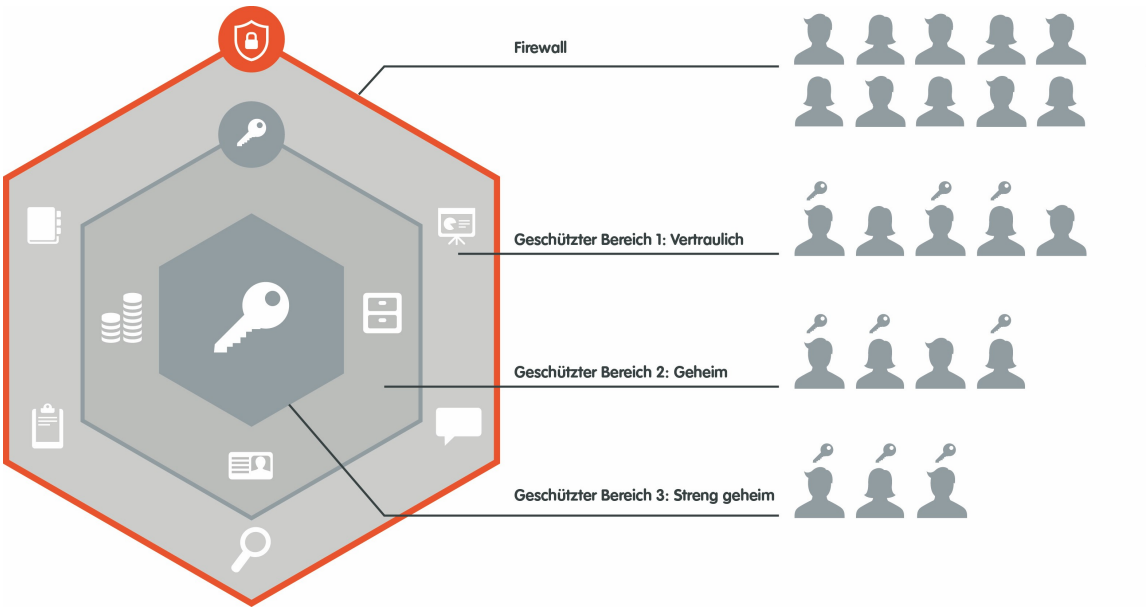
Verzeichnisebene

Wo hat wer Zugriff?

Entscheidungsebene

Wer sollte worauf Zugriff haben?

Access Rights Management verhindert den unbefugten Zugriff auf Daten und optimiert sicherheitsrelevante Prozesse innerhalb des Firmennetzwerks.

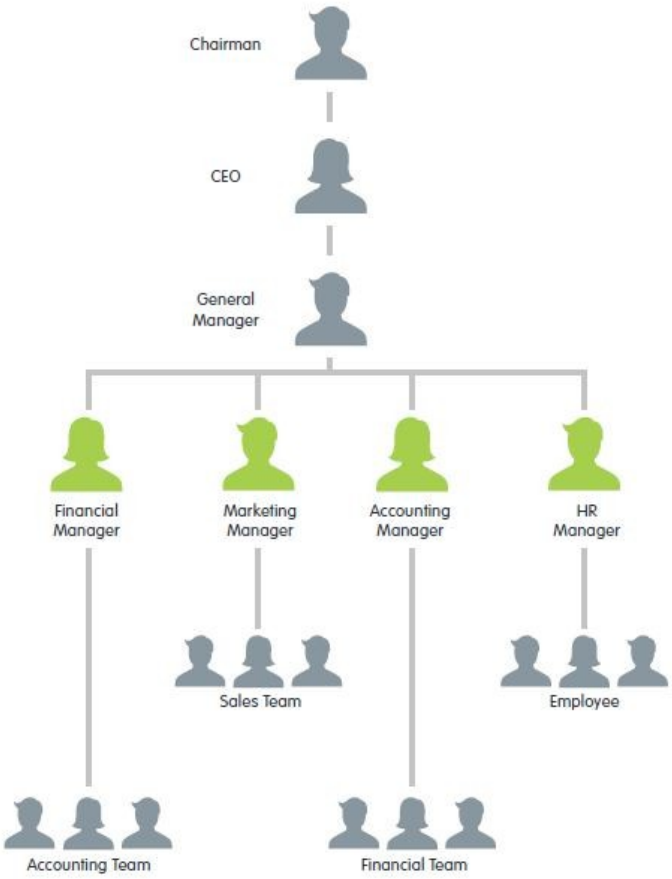


1.2 Um Sicherheitskompetenz zu dezentralisieren

Sicherheitsbeauftragte wissen nicht, wo wichtige Daten liegen und wer darauf zugreifen darf.

8MAN Access Rights Management delegiert diese Aufgabe an die Entscheider in Ihrer Firma. Diese vergeben Zugriffsrechte und tragen Sicherheitskompetenz in Ihr Unternehmen.

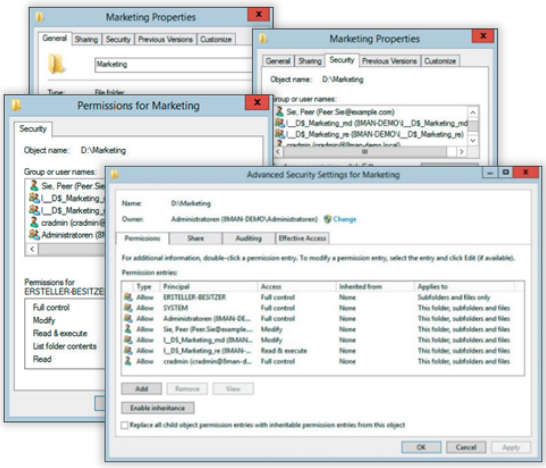
Mit 8MAN werden Führungskräfte zu Datenschützern:



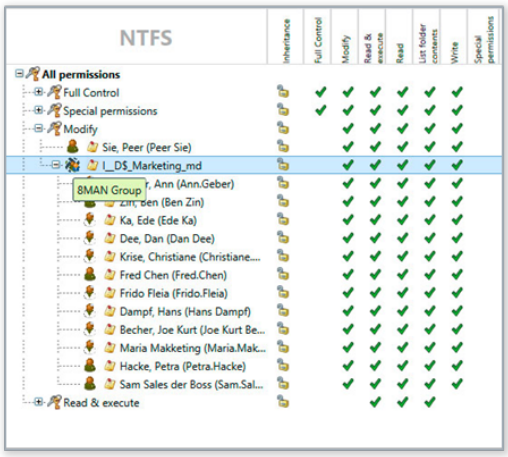
1.3 Damit Sicherheit effizient wird

Sicherheitsmaßnahmen werden nicht ausgeführt, wenn sie ineffizient sind. Access Rights Management automatisiert Prozesse und vereint zwei Gegner: Sicherheit + Effizienz.

Die Zugriffsrechteverwaltung mit Bordmitteln:



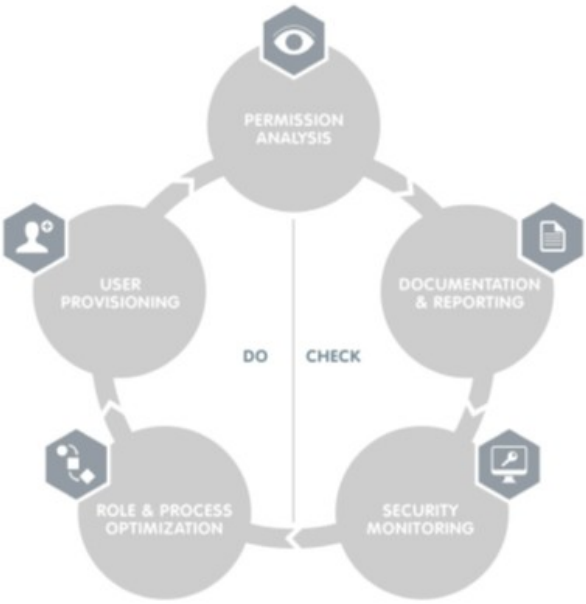
8MAN Access Rights Management:



8MAN Access Rights Management macht Sicherheit erst möglich:

Aufgabe	Arbeit mit Bordmitteln	Mit 8MAN
Erfassung der Berechtigungssituation in Ihrem Firmennetzwerk.	n/a	3 Minuten
Änderungen der Berechtigungssituation nachvollziehen.	n/a	2 Minuten
Prozesstransparenz bei sicherheitsrelevanten Aktionen im Firmennetzwerk.	n/a	2 Minuten
Ausführung von Standardprozessen: User Provisioning, Dokumentation und revisionssichere Reporte.	Auf Zuruf uneinheitlich und zeitintensiv	Automatisiert, standardisiert und schnell.

2. Die 5 Kerndisziplinen des ARM



8MAN Access Rights Management basiert auf fünf zentralen Disziplinen:

PERMISSION ANALYSIS

Zeigt ressourcenübergreifend die Berechtigungssituation in Ihrem Unternehmen.

DOCUMENTATION & REPORTING

Erfasst Access Rights Aktivitäten im Logbuch und erstellt Reporte.

SECURITY MONITORING

Überwacht sicherheitsrelevante Prozesse im Active Directory und auf Ihren Fileservern.

ROLE & PROCESS OPTIMIZATION

Verkürzt Ihren Access Rights Management Prozess und involviert nur die notwendigen Akteure.

USER PROVISIONING

Regelt die Anlage neuer Nutzerkonten, die Rechteverwaltung und die Bearbeitung von Kontodetails.

2.1 Permission Analysis

8MAN analysiert die Berechtigungslage in Ihrem Unternehmen und zeigt, wer auf welche Ressourcen zugreifen kann. In einer zentralen Ansicht sehen Sie die Gruppenmitgliedschaften aus dem Active Directory und die Zugriffsrechte für Ihre Fileserver, SharePoint Sites, Exchange und weiterer Technologien. Mit diesem Wissen sind Sie in der Lage, zu handeln und Ihr Unternehmen vor internen Sicherheitsvorfällen zu schützen.

Darüber hinaus zeigt 8MAN Ihnen die gefährliche Sicherheitslücken: Direktberechtigungen, unaufgelöste SIDs und Rekursionen lassen sich schnell identifizieren und entfernen.

Zu den Services

Hinweis zu den Produktversionen:

Permission Analysis ist in jeder 8MAN Version für Active Directory und Fileserver enthalten.

Möchten Sie weitere Ressourcen mit 8MAN analysieren, empfehlen wir den Zukauf folgender Add-Ons:

8MATE for Exchange

8MATE for SharePoint

2.2 Documentation & Reporting

Damit ihre IT revisionssicher arbeitet ist Dokumentation unerlässlich. Deshalb speichert 8MAN Eingriffe in die Berechtigungsstruktur automatisch für Sie ab. Jede Aktion erfordert die Hinterlegung eines Kommentars. Damit lässt sich im Nachhinein rekonstruieren, weshalb eine Aktion durchgeführt wurde. Die Berechtigungssituation ist nicht nur für technisch versierte Administratoren interessant. Unsere Reporte zeigen sehr einfach und strukturiert wer wo Zugriff hat. Damit erfüllt 8MAN die zentralen Anforderungen von IT-Sicherheitsregularien und dem Datenschutz.

Zu den Services

Hinweis zu den Produktversionen:

Documentation und Reporting ist in jeder 8MAN Version für Active Directory und Fileserver enthalten.
Möchten Sie weitere Ressourcen mit 8MAN dokumentieren, empfehlen wir den Zukauf folgender Add-Ons:
8MATE for Exchange
8MATE for SharePoint

2.3 Security Monitoring

Sowohl im Active Directory als auch auf dem Fileserver führen eine Reihe von Mitarbeitern Änderungen aus. Ohne ein vollumfängliches Monitoring entstehen Sicherheitsrisiken. Mit den 8MATEs AD Logga (für Active Directory), FS Logga (für Fileserver) und Exchange Logga, erfassen Sie sicherheitsrelevante Aktivitäten in Ihrem Firmennetzwerk. Damit können Sie nachvollziehen, wer was wann im Netzwerk gemacht hat und bei Problemen die Ursachen aufklären.

Auf Prozessebene erlangen Sie vollständige Transparenz über die Access Rights Aktivitäten. Selbst außerhalb von 8MAN vorgenommene Änderungen werden erfasst. Auf Basis der gewonnenen Informationen lässt sich Ihr Access Rights Management Prozess optimieren. Mit den Alerts (in FS und AD Logga enthalten) werden Sie bei kritischen Ereignissen proaktiv informiert.

Das Security Monitoring ist mit jeder Basisversion kombinierbar. Es basiert auf drei kostenpflichtigen Add-Ons:

Active Directory

8MATE AD Logga

Fileserver

8MATE FS Logga

Exchange

8MATE Exchange Logga

2.4 Role & Process Optimization

Nicht der Administrator sondern ein Data Owner bzw. Vorgesetzter weiß am besten, wer worauf Zugriff haben sollte. Mit der Einführung eines Rollenkonzeptes für die Analyse und Erteilung von Zugriffsrechten tragen Sie den Data Awareness Gedanken und entsprechendes Handeln in Ihr Unternehmen. Mit dem Data Owner Konzept von 8MAN bilden Sie das Organigramm Ihrer Firma nach und erfassen alle Abteilungen. Anschliessend weisen Sie den einzelnen Data Owners ihre Mitarbeiter zu. Die Data Owners analysieren oder vergeben die Zugriffsrechte Ihrer Mitarbeiter auf Ressourcen. Standardoperationen wie z. B. das Zurücksetzen eines Kennwortes kann mit 8MAN der Helpdesk erledigen.

Hinweis zu den Produktversionen:

Role & Process Optimization benötigt die Basisversion "Enterprise".

Möchten Sie den Access Rights Management Prozess über das GrantMA Self-Service Portal steuern, benötigen Sie den 8MATE GrantMA.

8MATE GrantMA

Komplexe Freigabeworkflows abbilden

Workflows für Mitarbeiter

Zu den Services

2.5 User Provisioning

8MAN bietet User Provisioning in seiner elementaren Form. Mit Hilfe von rollenspezifischen Templates legen Sie neue Benutzer innerhalb von Sekunden an. Die Nutzergenerierung erfolgt standardisiert und entsprechend der Rollen in Ihrem Unternehmen. Die in den Active-Directory-Gruppen definierten Zugriffsrechte für Fileserver, SharePoint Sites, Exchange und virtuelle Server werden gleich mit vergeben.

Damit der neue Kollege gleich starten kann, generiert 8MAN das passende Mail-Konto. Terminieren Sie die Aktivierung, um den Eintritt in der Zukunft vorzubereiten oder bei Projektarbeiten zeitlich zu begrenzen. Ob Helpdesk oder Data Owner: In beiden Fällen arbeiten die Beteiligten mit einem reduzierten, einfachen Interface. Alle Zugänge sind in wenigen Schritten gelegt.

Zu den Services

Hinweis zu den Produktversionen

User Provisioning benötigt die Basisversion "Enterprise".

Möchten Sie weitere Ressourcen mit 8MAN administrieren, empfehlen wir den Zukauf folgender Add-Ons:

8MATE for Exchange

8MATE for SharePoint

3. Weitere ARM Disziplinen

Threat & Gap Management

Entfernt sicherheitskritische Berechtigungsfehler automatisch und standardisiert das Rechtesystem nach Ihren Vorgaben.

8MAN Ressource Integration

Ermöglicht die Administration weiterer Ressourcen.

8MAN Application Integration

Ermöglicht die automatisierte Zusammenarbeit mit anderen Applikationen in Ihrer Softwarelandschaft.

3.1 Resource Integration

8MAN Resource Integration

Ermöglicht die Analyse und Administration weiterer Ressourcen.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 4.499 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen.

3.1.1 +8MATE for Exchange

Problem

Die Verwaltung von Berechtigungen mit Microsoft Exchange ist komplex. Die Microsoft Boardmittel erlauben keine ganzheitliche Sicht auf Zugriffsrechte von öffentlichen Ordnern und Postfächern. Auch die Administration der Zugriffsrechte ist umständlich und zeitintensiv.

Lösung

Mit dem 8MATE for Exchange erweitern Sie ihren 8MAN für Emailressourcen. Damit erfolgt die Analyse und Administration von Berechtigungen zentral und im Einklang mit dem Access Management für andere Anwendungen. In der gewohnten 8MAN Übersicht sehen Sie auf einen Blick, wer auf öffentliche Ordner, Postfächer, Postfachordner und z.B. Kalender zugreifen kann.

Die Administration von Exchange ist eng an den Onboarding-Prozess angelegt: Die Anlage von Postfächern und Vergabe von Zugriffsrechten erfolgt direkt im 8MAN. Änderungen werden revisionssicher im 8MAN dokumentiert.

Neben der Analyse und Administration von Berechtigungen im Exchange verfügt der 8MATE über weitere Features:

- Erstellung von Abwesenheitsnotizen ohne Zugriff auf das Emailkonto
- Auflistung von Stellvertretern für Postfächer und Send As Berechtigungen
- Administration von Postfachgrößen

3.1.2 +8MATE for SharePoint

Problem

Die Analyse und Verwaltung von Berechtigungen auf SharePoint ist komplex.

Die Microsoft Boardmittel erlauben keine ganzheitliche Sicht auf die Zugriffsrechte einzelner SharePoint-Ressourcen. Auch die Administration von Berechtigungen ist umständlich und zeitintensiv. Vorgenommene Änderungen in der Berechtigungsstruktur sind nicht nachvollziehbar.

Lösung

Der 8MATE for SharePoint integriert sämtliche SharePoint-Ressourcen in Ihren 8MAN. Damit erfolgt die Analyse und Administration von Berechtigungen zentral und im Einklang mit dem Access Management für andere Anwendungen. Sie profitieren von der Analyse- und Darstellungskompetenz des 8MAN und können Zugangsrechte schnell verändern.

8MAN zeigt die Berechtigungen in einer Baumstruktur an. Damit sehen Sie schnell, wer auf welche SharePoint Ressource zugreifen kann. Über den Scanvergleich-Report erfahren Sie, wer welche Änderungen an Berechtigungen durchgeführt hat und erhalten ein Protokoll vorgenommener Aktivitäten für die Revision.

Mit dem 8MATE for SharePoint können Sie in der 8MAN Oberfläche alle Berechtigungen vergeben. Mit dem Group Wizard und der Vergabe von Namenskonventionen standardisieren Sie Ihren Berechtigungsvergabeprozess.

3.1.3 +8MATE for Dynamics NAV

Problem

Microsoft Dynamics NAV beinhaltet unternehmerische Informationen, die nicht jeder sehen sollte. Je nach Ausbaustufe der ERP-Lösung sind dort Projektbudgets, EK-Preislisten, Jahresbilanzen oder personenbezogene Daten von Mitarbeitern, Lieferanten oder Kunden hinterlegt.

Ein effizientes Berechtigungsmanagement ist mit Bordmitteln schwierig. Nutzer sind Mitglied in verschiedenen Berechtigungsgruppen, die wiederum Mitglied in weiteren Berechtigungsgruppen sein können. Darüber hinaus nutzt die ERP-Lösung unternehmensspezifische Berechtigungssätze, über die ebenfalls Zugriffsrechte vergeben werden. Möchte man wissen, welche Nutzer welche Zugriffsrechte haben, müssen entsprechend viele Quellen konsolidiert werden. Die Antwort auf die eigentlich sehr einfache Frage: „Wer hat wo Zugriff?“, wird zu einem kostspieligen und zeitintensiven Suchprojekt.

Lösung

Das 8MATE Dynamics NAV integriert die Berechtigungsanalyse des ERP-Systems in 8MAN. In gewohnter Weise sehen Sie alle Zugriffsrechte in einer flachen Liste. Im ersten Schritt bietet das Modul Services im Bereich Permission Analysis und Documentation & Reporting:

Permission Analysis

- Zugriffsrechte auf NAV Ressourcen identifizieren
- Mehrfachberechtigungen identifizieren
- Die Berechtigungssituation aus der Vergangenheit analysieren

Documentation & Reporting

- Report: Wer hat wo Zugriff?
- Report: Wo haben Benutzer/Gruppen Zugriff?

3.1.4 Easy Connect - beliebige Ressourcen in 8MAN einbinden

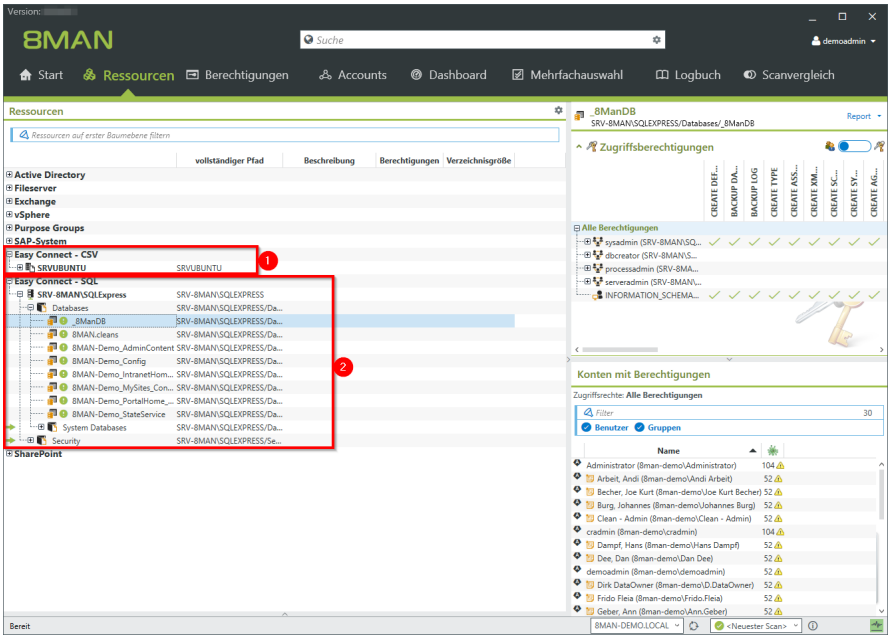
Hintergrund / Mehrwert

Mit Easy Connect binden Sie weitere Ressourcensysteme in 8MAN ein. Sie gewinnen so die 8MAN-typische Übersicht über die Berechtigungslage für diese Systeme. Die Frage "Wo hat ein Benutzer Zugriff" kann somit noch umfassender und einfacher beantwortet werden. Die Daten werden z.B. über ein CSV-Format importiert oder per SQL-Script aus einer (Berechtigungs-)Datenbank ausgelesen.

Folgende Reporte werden für Easy Connect Ressourcen unterstützt:

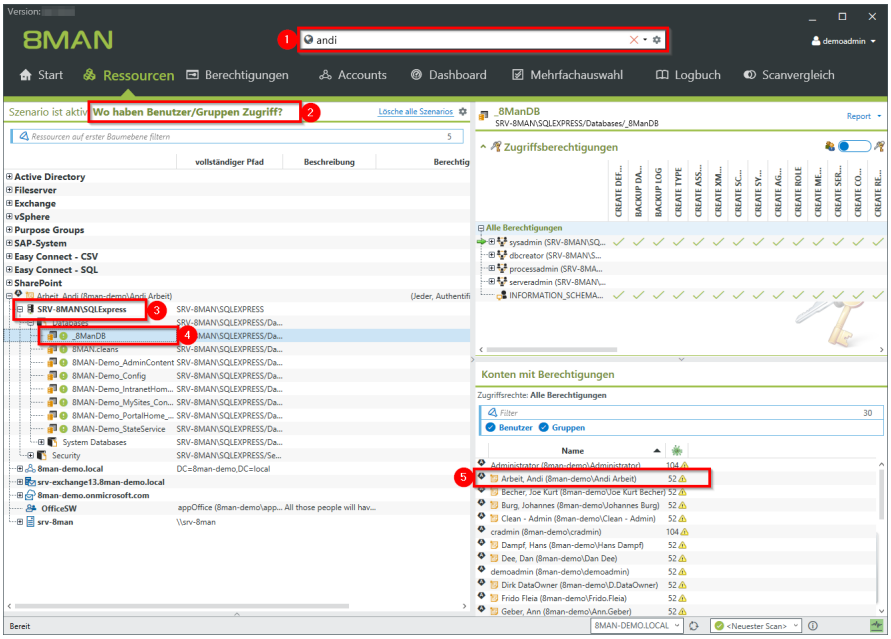
- "Wer hat wo Zugriff?"
- "Wo hat ein Benutzer/Gruppe Zugriff?"
- "Konto-Details"

3.1.4.1 Easy Connect Ressourcen in 8MAN anzeigen



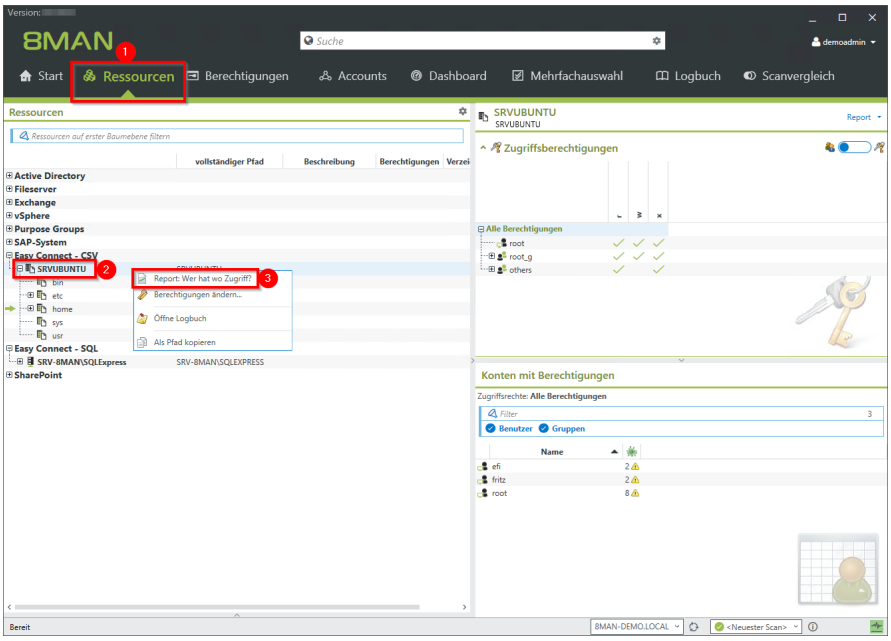
Im hier gezeigten Beispiel wurden die Berechtigungsinformationen eines Linux-Dateisystems und eines MS SQL-Servers importiert.

1. *Die Berechtigungsinformationen des Linux-Dateisystems wurden per CSV importiert.*
2. *Die Berechtigungsinformationen des SQL-Servers wurden per SQL-Script aus der Datenbank ausgelesen.*

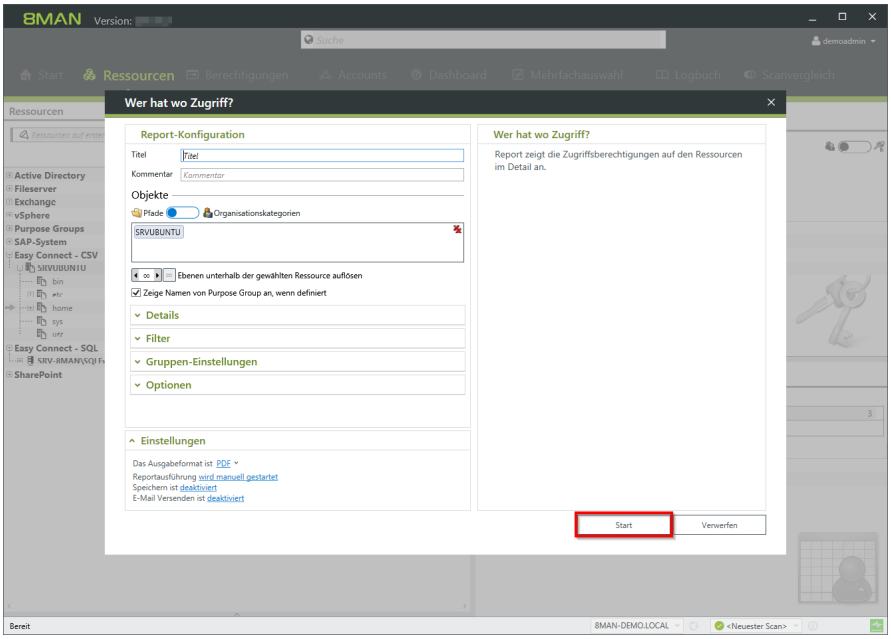


1. *Die Suche umfasst die mit Easy Connect eingebundenen Ressourcen.*
2. *Das Szenario "Wo haben Benutzer/Gruppen Zugriff?" schließt die Easy Connect Ressourcen mit ein.*
3. *Die importierte SQL-Server-Ressource ist im Szenario enthalten.*
4. *Navigieren Sie innerhalb der Easy Connect Ressourcenstruktur.*
5. *In der 8MAN-typischen Übersicht sehen Sie die Berechtigungen für den gewünschten Benutzer.*

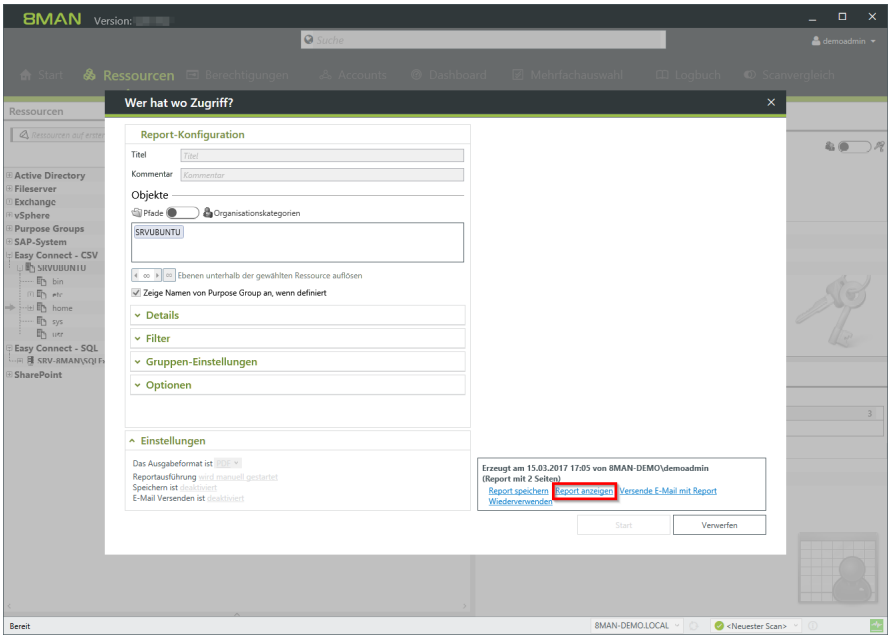
3.1.4.2 Einen Report für Easy Connect Ressourcen erstellen



1. *Wählen Sie die Ansicht "Ressourcen".*
2. *Selektieren Sie die gewünschte Ressource.*
3. *Wählen Sie "Report: Wer hat wo Zugriff?" aus dem Kontextmenü nach Rechtsklick.*



Starten Sie den Report.



Klicken Sie auf Report anzeigen.

3.2 8MAN Application Integration

Application Integration

Ermöglicht die automatisierte Zusammenarbeit mit anderen Applikationen in Ihrer Softwarelandschaft.

3.2.1 +8MATE Matrix 42

Der 8MATE Matrix42 verknüpft 8MAN mit der IT Service Management Lösung Matrix42. In der von der Futuredat GmbH entwickelten Lösung bestellen Mitarbeiter im Self-Service Portal von Matrix42 Fileserver-Berechtigungen.

Data Owners bzw. Administratoren prüfen die Bestellung in einem standardisierten Prozess. Bei Bewilligung wird 8MAN automatisch aktiv und erstellt die Berechtigung auf dem Fileserver. Dies erfolgt nach Microsoft Best Practice über Active-Directory-Gruppen. Der Prozess wird sowohl in Matrix42 als auch vom 8MAN Logbuch automatisch dokumentiert.

3.3 Threat & Gap Management

Threat & Gap Management

Entfernt sicherheitskritische Berechtigungsfehler automatisch und standardisiert das Rechtesystem nach Ihren Vorgaben.

3.3.1 8MATE Clean!

Problem

Die Korrektur von Berechtigungsfehlern und Inkonsistenzen ist auf Fileservern nur schwer möglich. Die Umsetzung von Best Practices scheitern an zwei zentralen Hürden: Wissen und Zeit. Darüber hinaus liegt der Fokus im klassischen Access Rights Management (ARM) auf der Verzeichnisebene. Sie ist die zentrale Analyseebene, blendet aber die Dateiebene aus.

Lösung

8MATE Clean! startet einen Prozess, der in einen sicheren und standardisierten Fileserver mündet. Durch eine Reihe klarer Entscheidungen definieren Sie, wie mit Sicherheits- und Strukturproblemen umgegangen werden soll. Ihre Anforderungen und die in 8MAN hinterlegten Best Practices werden automatisch umgesetzt. Darüber hinaus ist die Archivierung veralteter Daten möglich. Denn: Je geringer die Dateimasse, desto einfacher die Verwaltung.

Was bewirkt der 8MATE Clean! ?

- Archiviert alte Fileserver - Dateien
- Entfernt kritische Berechtigungen automatisch
- Entfernt oder ersetzt Direktberechtigungen
- Standardisiert vorhandene Berechtigungsarten auf Ihren Fileservern

Der 8MATE Clean wird ausschließlich in Kombination mit Professional Services ausgeführt.

4. Permission Analysis

4.1 Active Directory

Active Directory ist das führende System für die Administration von Windows Netzwerken. 8MAN konzentriert sich einerseits auf die Analyse der Konten und Gruppen und andererseits um die Erstellung und Bearbeitung ebendieser. Dies erfolgt domänen- und gesamtstrukturübergreifend. Über den Group Wizard legt 8MAN automatisch Berechtigungsgruppen im Active Directory an.

4.1.1 Services für Administratoren

4.1.1.1 Gruppenverschachtelungen visualisieren

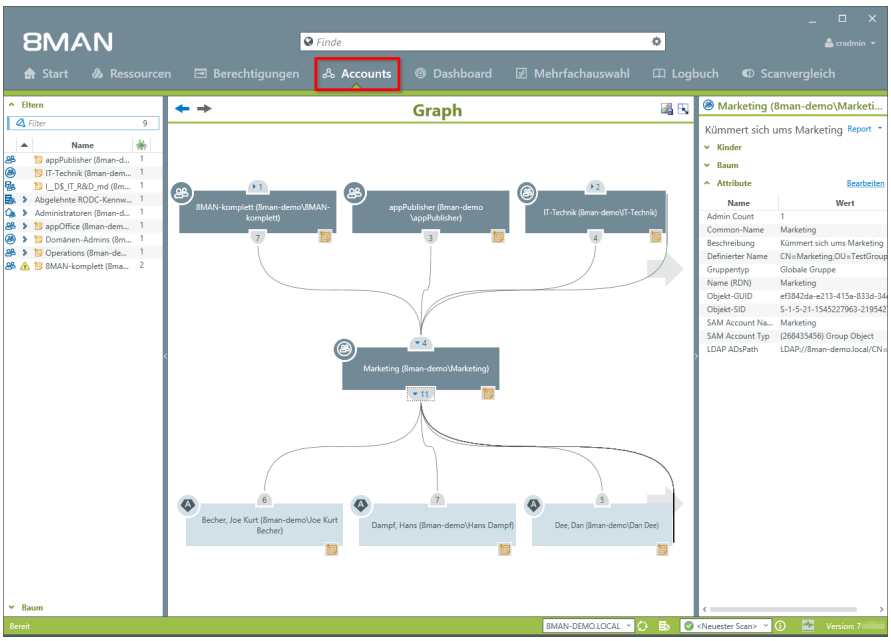
Hintergrund / Mehrwert

Zentraler Bestandteil jedes Active Directory (AD) ist das Gruppenkonzept. Administratoren nutzen Gruppen, um Zugriffsrechte und Ressourcen einzelnen Nutzern oder Nutzergruppen zuzuweisen. Dadurch entstehen Verschachtelungen: Beispielsweise gibt die Gruppe "Marketing" Zugriffsrechte auf die entsprechenden Fileserververzeichnisse der Abteilung. Gleichzeitig ist die Gruppe aber auch Mitglied (also verschachtelt) mit der Gruppe "Zugang Wlan 4.Etage". Der 8MAN AD Graph zeigt die Verschachtelungsstruktur in Ihrem Active Directory und hilft Ihnen dabei gewachsene Strukturen zu erkennen und Strukturfehler anzupassen.

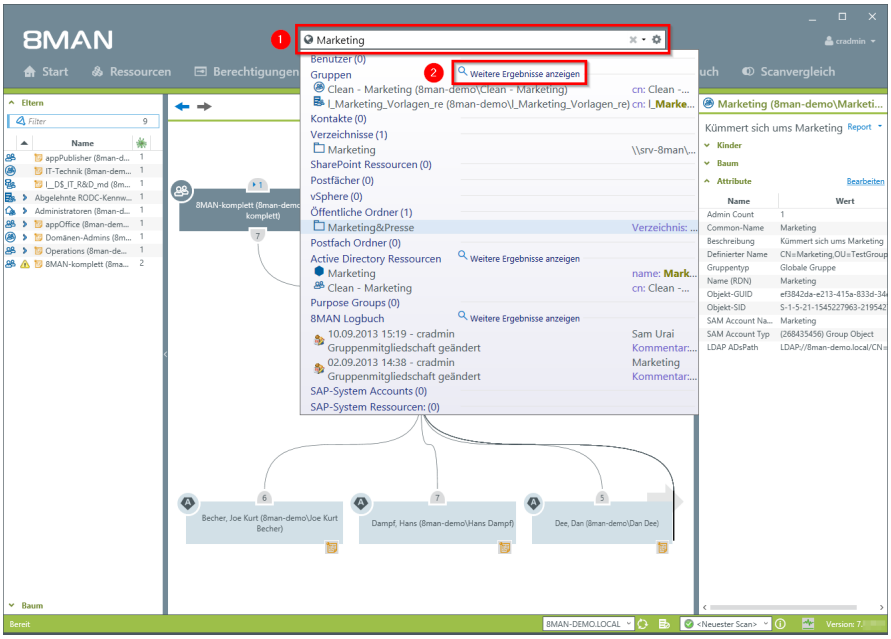
Weiterführende Services

Extreme Verschachtelungstiefen im AD identifizieren
Rekursive Gruppen identifizieren

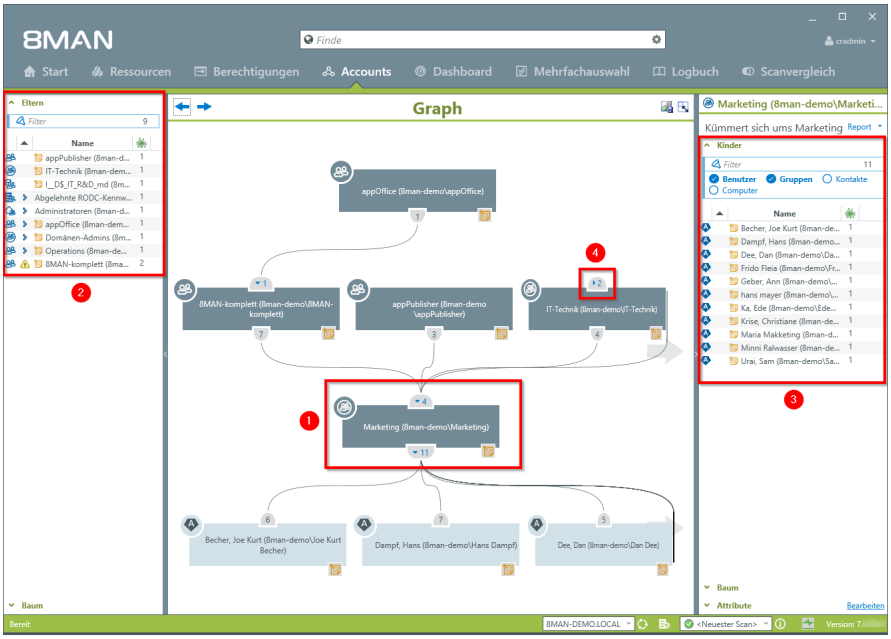
Der Prozess in einzelnen Schritten



Wechseln Sie in die Accounts-Ansicht.



1. *Finden Sie über das Suchfeld die AD Gruppe. Im Beispiel "Marketing". Klicken Sie im Suchergebnisfeld "Gruppen" auf das gewünschte Ergebnis.*
2. *Sie finden Ihre Ressource nicht? Klicken Sie auf "Weitere Ergebnisse anzeigen".*



1. *Die Gruppe "Marketing" ist im Fokus Ihrer Analyse.*
2. *Oberhalb der Gruppe sehen Sie im Graph die vier Gruppen, in denen die Gruppe "Marketing" Mitglied ist - die sogenannten "Eltern". Links in einer flachen Liste sind alle "Eltern" aufgeführt, sowohl direkte als auch indirekte. Indirekte "Eltern" sind durch den blauen Pfeil gekennzeichnet.*
3. *Unterhalb der Gruppe im Graph und auf der rechten Seite (flache Liste) sehen Sie alle "Kinder" der Gruppe - direkte und indirekte.*
4. *Klappen Sie Äste auf oder zu. An der Ziffer lesen Sie ab, wie viele direkte "Eltern" oder "Kinder" vorhanden sind.*

4.1.1.2 Berechtigungssituationen miteinander vergleichen (Scanvergleich)

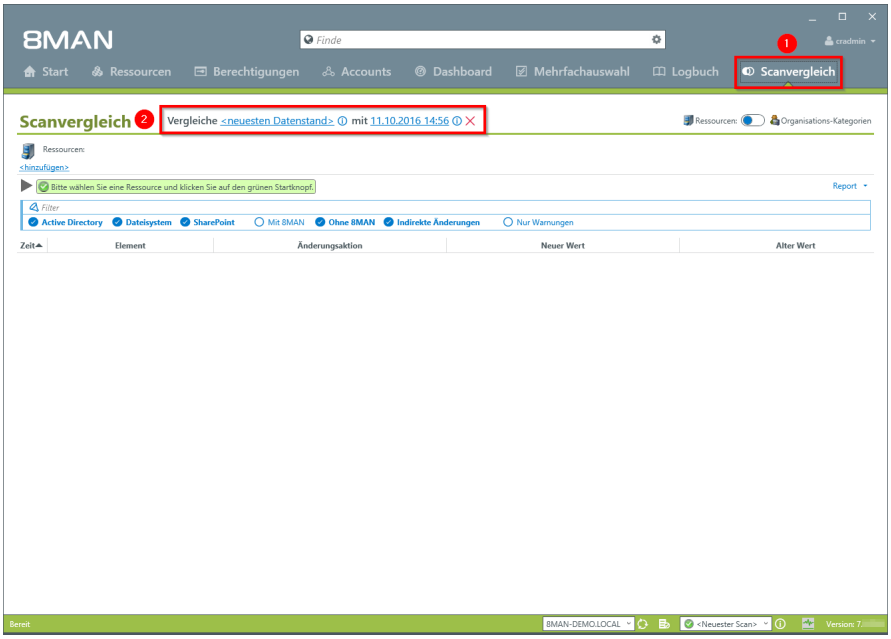
Hintergrund / Mehrwert

Der Scan-Vergleich zeigt die IST-Zustände von zwei Berechtigungssituationen im AD und vergleicht diese miteinander. Sie können somit feststellen, inwieweit sich Ihre AD verändert hat.

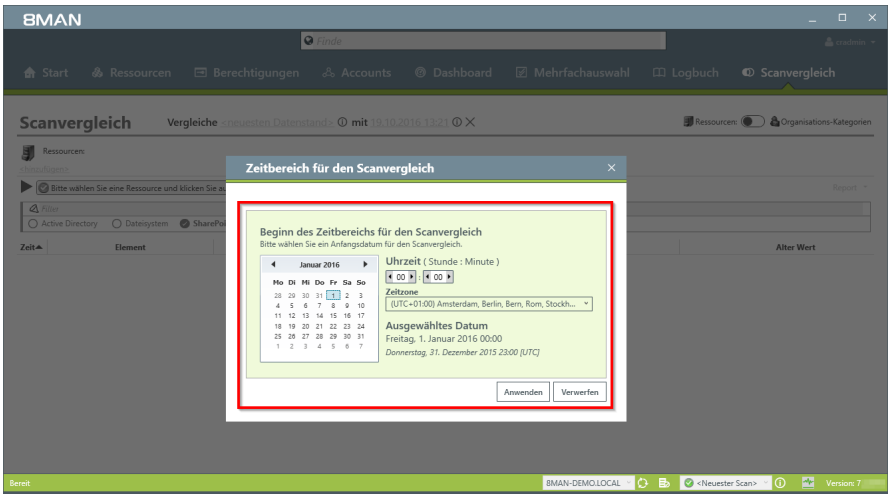
Weiterführende Services

Der Vergleich bezieht nur zwei Messzeitpunkte in die Analyse ein. Um den gesamten IST-Prozess eines Zeitraumes zu identifizieren, benötigen Sie den im Security Monitoring angebotenen 8MATE FS Logga.
Nutzen Sie alternativ zum Scan-Vergleich den Berechtigungsdifferenzreport.

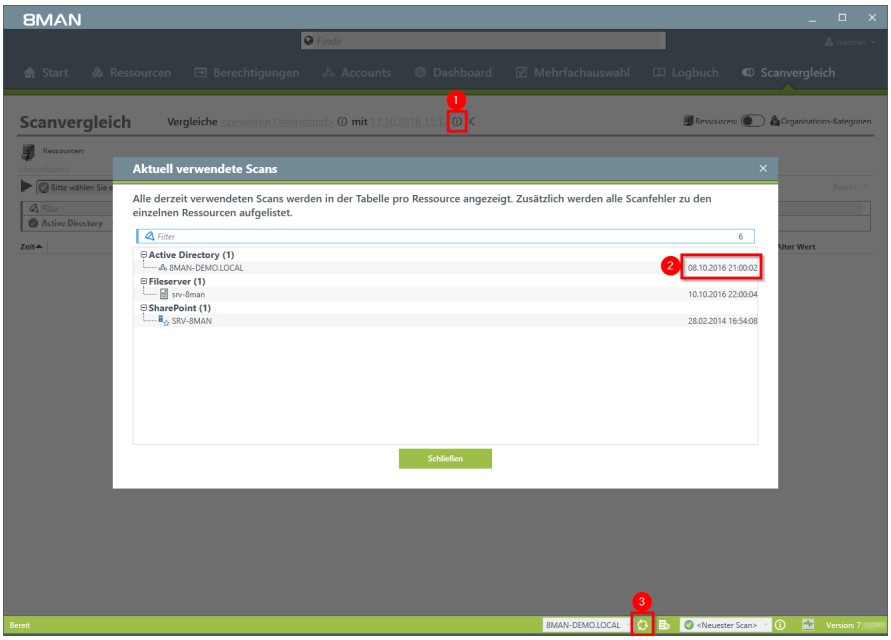
Der Prozess in einzelnen Schritten



1. *Klicken Sie auf den Menüpunkt "Scanvergleich".*
2. *Wählen Sie zwei Datenstände, die miteinander verglichen werden sollen.*

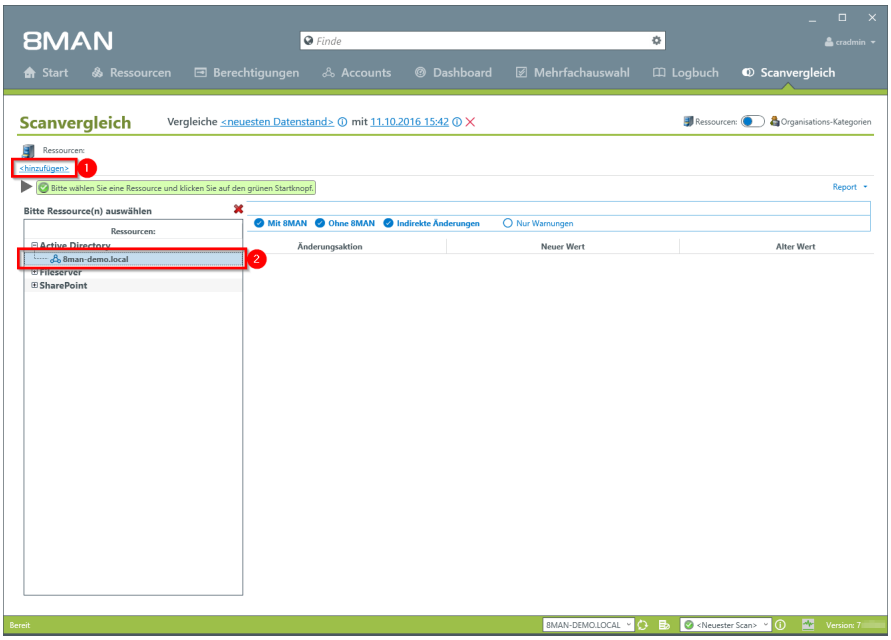


Wählen Sie Datum und Zeit für Anfang und Endpunkt.

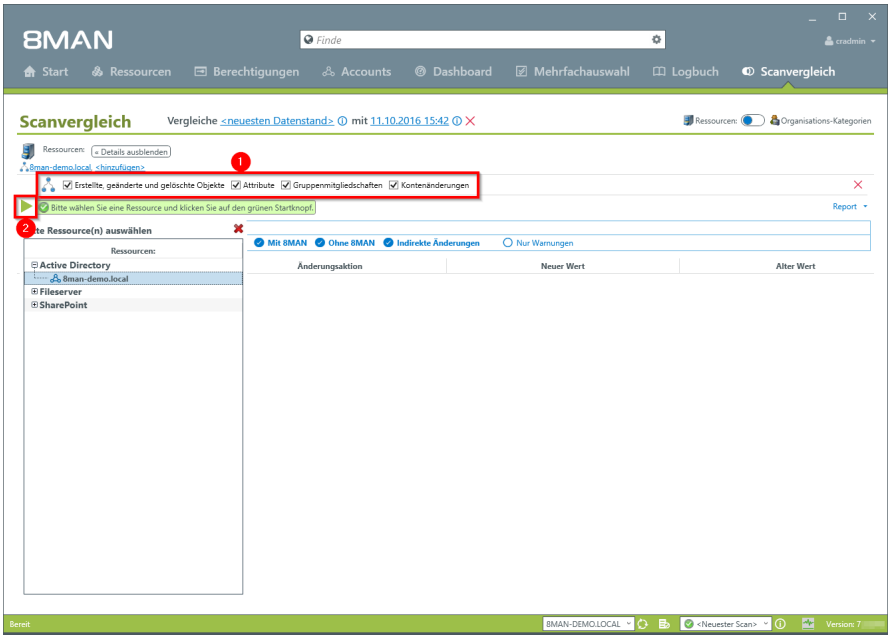


Der Vergleich bezieht sich immer auf vorhandene Scan-Datenstände.

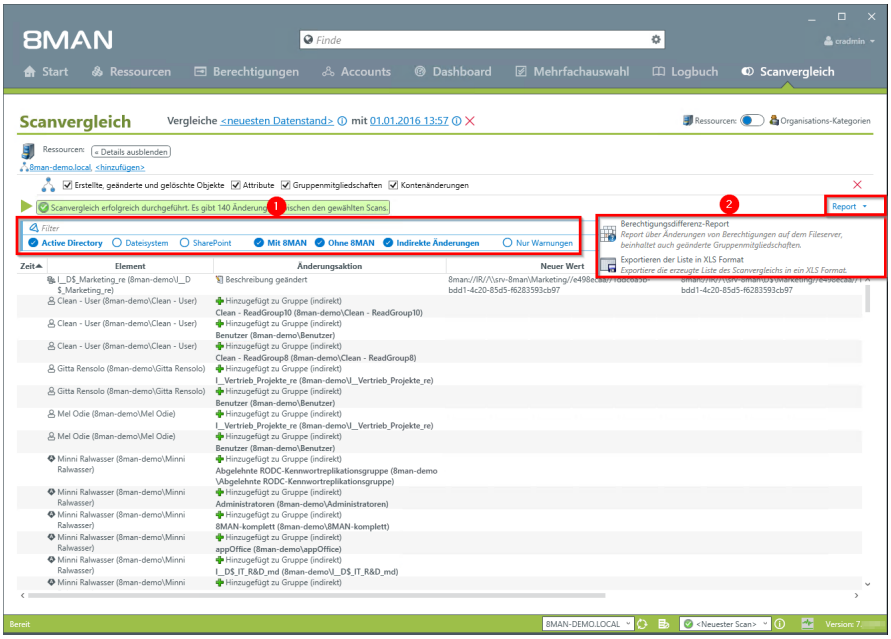
1. *Klicken Sie auf das Informationssymbol.*
2. *8MAN zeigt Ihnen, welcher Scan-Datenstand für den Vergleich verwendet wird.*
3. *Führen Sie für ein möglichst aktuelles Ergebnis vorher einen neuen AD-Scan aus.*



1. *Klicken Sie auf Ressourcen hinzufügen.*
2. *Fügen Sie die gewählte Ressource mit Doppelklick hinzu.*



1. *Bestimmen Sie den Umfang des Vergleichs.*
2. *Starten Sie den Vergleich.*



1. *Mit dem Filter grenzen Sie die Vergleichsergebnisse ein.*
2. *Generieren Sie einen strukturierten Berechtigungsdifferenzreport und / oder exportieren Sie die vorliegenden Ergebnisse als .XLS Datei.*

4.1.1.3 Überberechtigte Benutzer anhand des Kerberos Tokens identifizieren

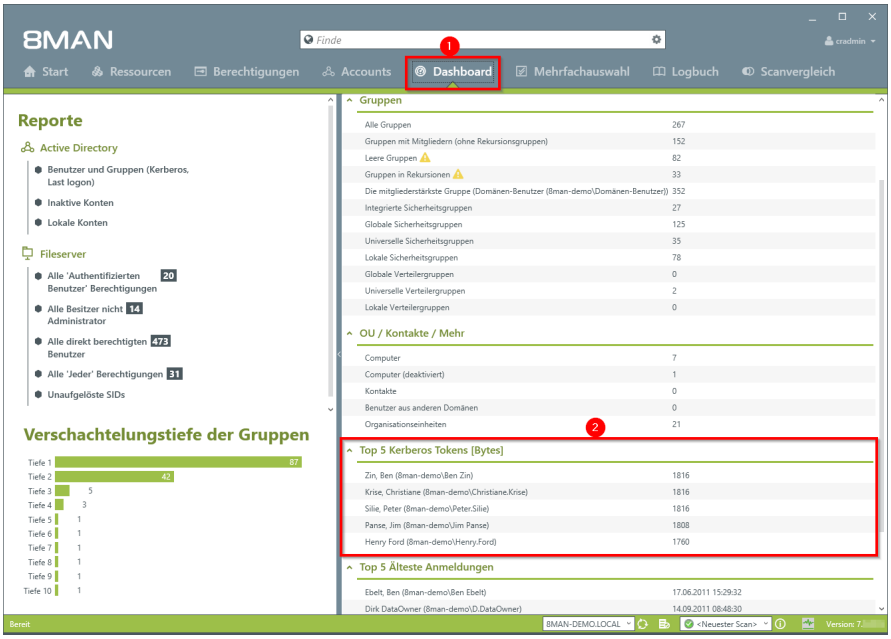
Hintergrund / Mehrwert

Die Größe des Kerberos Tokens ist ein guter Indikator, um Nutzer mit zu vielen Berechtigungen zu finden: Je mehr Gruppenmitgliedschaften ein User hat, desto größer ist sein Kerberos Token. Auch wenn nicht jede Gruppenmitgliedschaft automatisch Zugriffsrechte gibt, lohnt sich eine Analyse der gelisteten Nutzer.

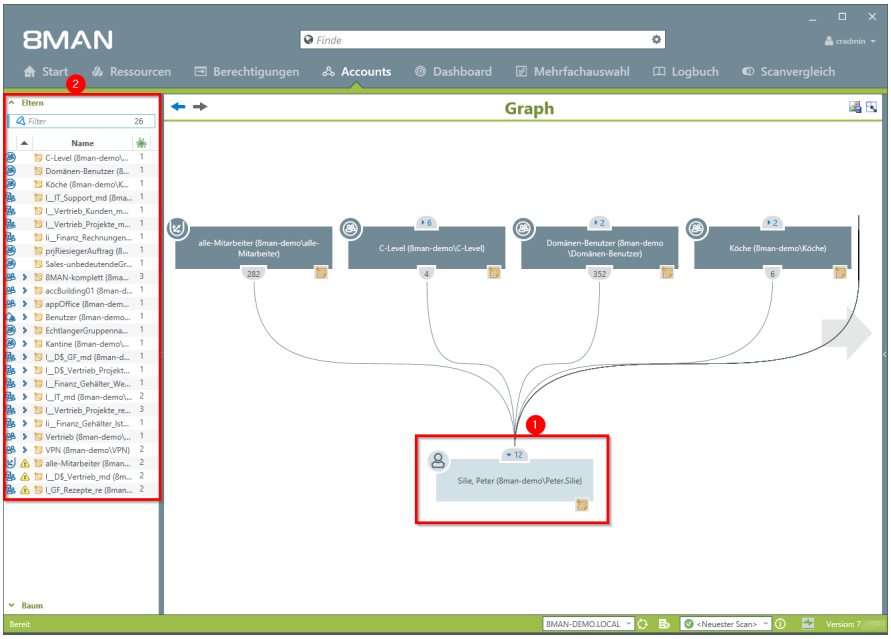
Darüber hinaus besteht die Gefahr, dass Nutzer mit zu vielen Gruppenmitgliedschaften sich nicht mehr anmelden können.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.8 Vergabe von Zugriffsrechten.

Der Prozess in einzelnen Schritten



1. *Wechseln Sie zum Dashboard.*
2. *Doppelklicken Sie auf die Nutzer im Bereich "Top 5 Kerberos Tokens".*



1. *8MAN wechselt automatisch in die Graph-Ansicht mit dem gewählten Benutzer im Fokus.*
2. *Auf der linken Seite sehen Sie alle "Eltern", also die Gruppen in denen der Nutzer direkt und indirekt Mitglied ist. Wir empfehlen die Nutzung der flachen Liste bei Nutzern mit extrem vielen Gruppenmitgliedschaften.*

4.1.1.4 Die Verschachtelungstiefe von Gruppen identifizieren

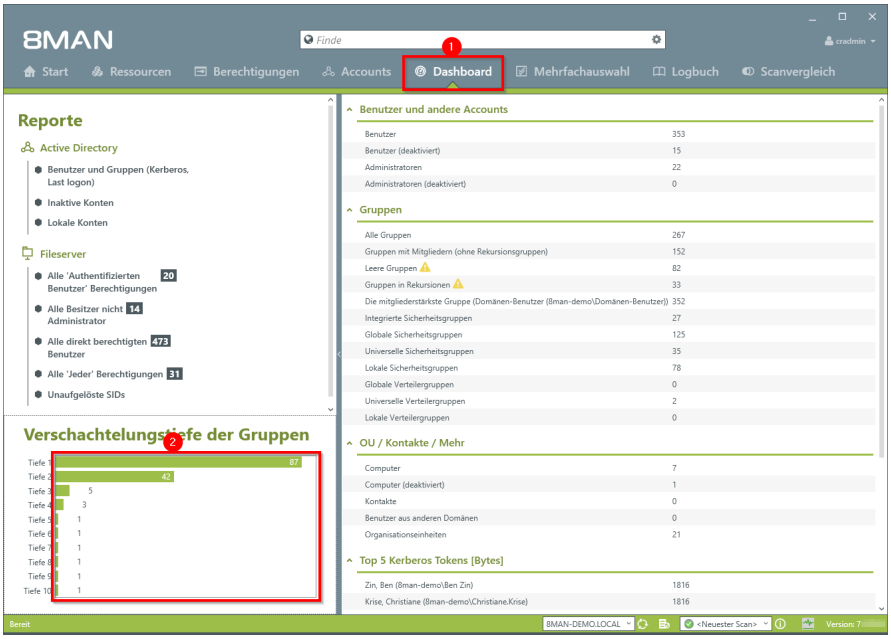
Hintergrund / Mehrwert

Ein über Jahre gewachsenes AD kann enorme Verschachtelungstiefen erreichen. Das 8MAN Dashboard zeigt Verschachtelungstiefen bis zur Ebene 10. Nach Microsoft Best Practice sollte Ihre AD maximal bis zur dritten oder vierten Ebene reichen. Identifizieren Sie die kritischen Bereiche Ihres AD und bauen dieses sukzessive um. Wir empfehlen eine flache Gruppenstruktur (d.h. mehr spezifische Gruppen konstruieren), da dadurch eine bessere Orientierung gewährleistet wird.

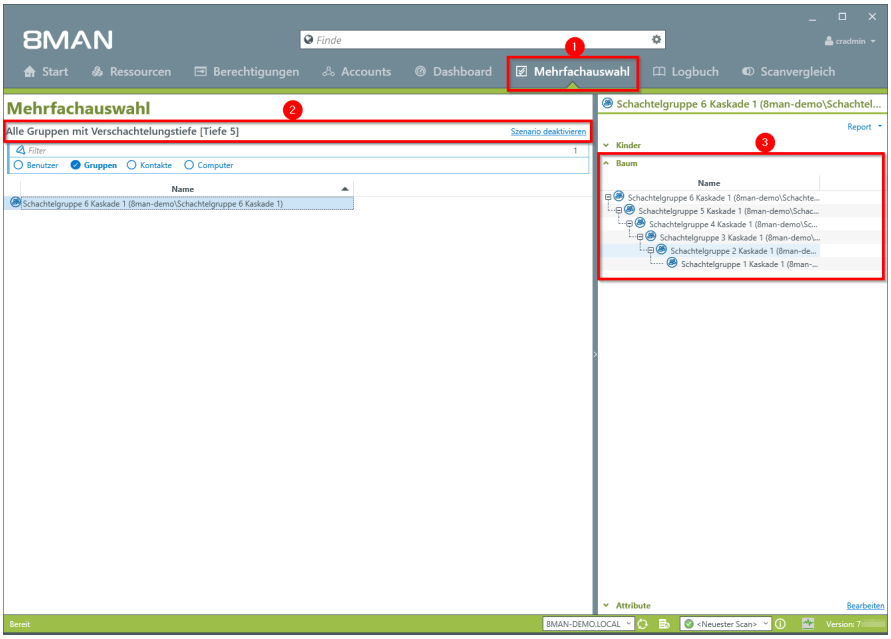
Weiterführende Services

Mehrere Gruppen auf eine Gruppe reduzieren

Der Prozess in einzelnen Schritten



1. *Wählen Sie das Dashboard.*
2. *Klicken Sie auf eine der Verschachtelungsebenen.*



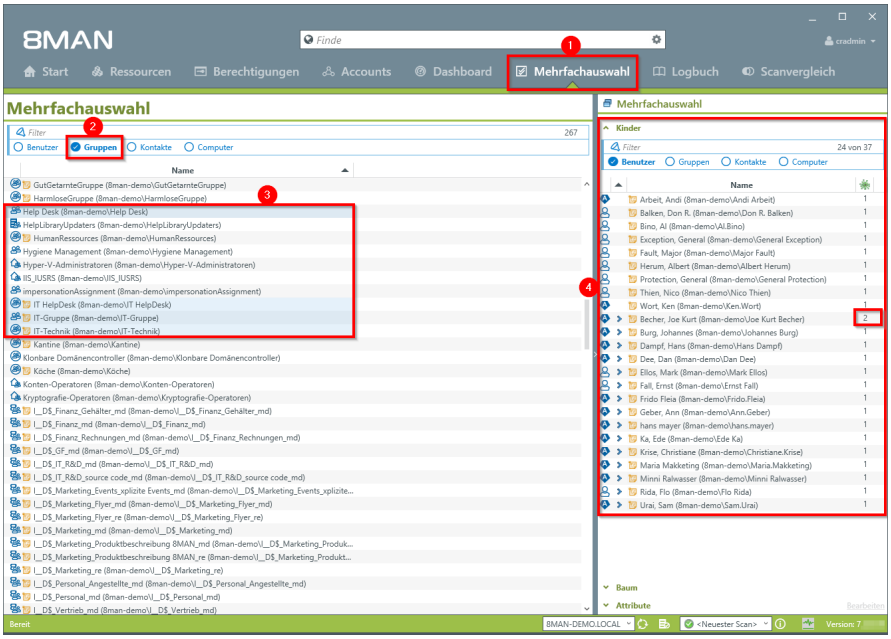
1. *8MAN springt automatisch in die Mehrfachauswahl.*
2. *Das aktivierte Szenario filtert automatisch nach Gruppen mit der entsprechenden Verschachtelungstiefe.*
3. *Lassen Sie sich die Verschachtelungen in einer Baumansicht anzeigen.*

4.1.1.5 Mitglieder unterschiedlicher Gruppen in einer Liste anzeigen

Hintergrund / Mehrwert

Mit der Mehrfachauswahl können Sie mehrere Gruppen markieren und damit eine Gesamtübersicht aller Mitglieder erhalten.

Der Prozess in einzelnen Schritten



1. *Wechseln Sie in die Mehrfachauswahl.*
2. *Filtern Sie nach Gruppen.*
3. *Markieren Sie die gewünschten Gruppen.*
4. *Erhalten Sie eine Gesamtübersicht ("Kinder") aller markierten Gruppen. Sind diese mehrfach enthalten, zeigt 8MAN dies an (z. B. bei Joe Kurt Becher).*

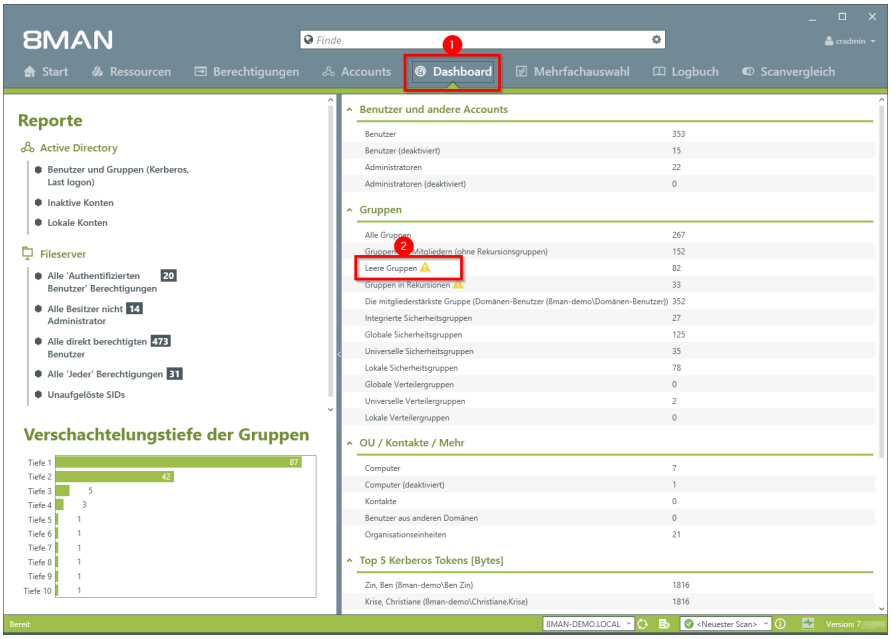
4.1.1.6 Leere Gruppen identifizieren

Hintergrund / Mehrwert

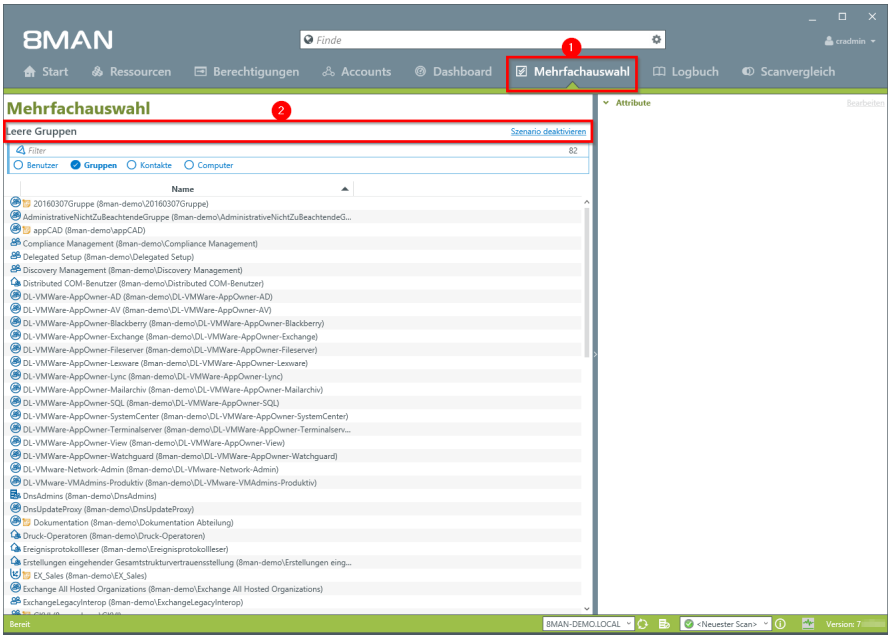
Im Active Directory sammeln sich über die Jahre leere Gruppen an. Diese verringern die Performance und behindern den Überblick.
Wir empfehlen diese Gruppen zu löschen.

Gruppen ohne Mitglieder können Systemgruppen sein. Diese sollten Sie nicht löschen.

Der Prozess in einzelnen Schritten



1. *Wechseln Sie zum Dashboard.*
2. *Doppelklicken Sie auf "Leere Gruppen".*



1. *8MAN wechselt automatisch in die Mehrfachauswahl.*
2. *Das Szenario "Leere Gruppen" ist aktiv. Die aufgelisteten Gruppen sind leer.*

4.1.1.7 Rekursive Gruppen identifizieren

Hintergrund / Mehrwert

Gruppen können Mitglieder von Gruppen sein. Active Directory lässt es zu, dass Kinder auch wieder Eltern im eigenen „Stammbaum“ werden. Schliessen sich die Verschachtelungen im Kreis, entstehen unsinnige Zirkelbezüge.

Durch diese sogenannten Rekursionen (engl. "circular nested groups") erhält jeder Benutzer, der in irgendeiner der verschachtelten Gruppen Mitglied ist, die Rechte aller beteiligten Gruppen. Die Folge ist eine unübersichtliche und schwer zu identifizierende Überberechtigung. 8MAN identifiziert automatisch alle Rekursionen in Ihrem System. Wir empfehlen diese zu unterbrechen.

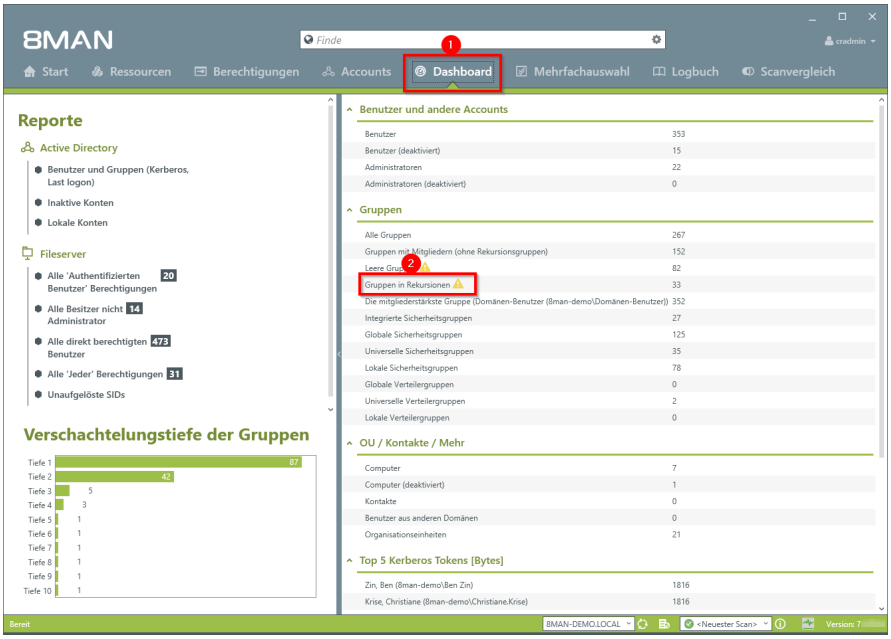
TIP: Administrieren Sie nur noch mit 8MAN und Rekursionen können nicht mehr entstehen.

Weiterführende Services

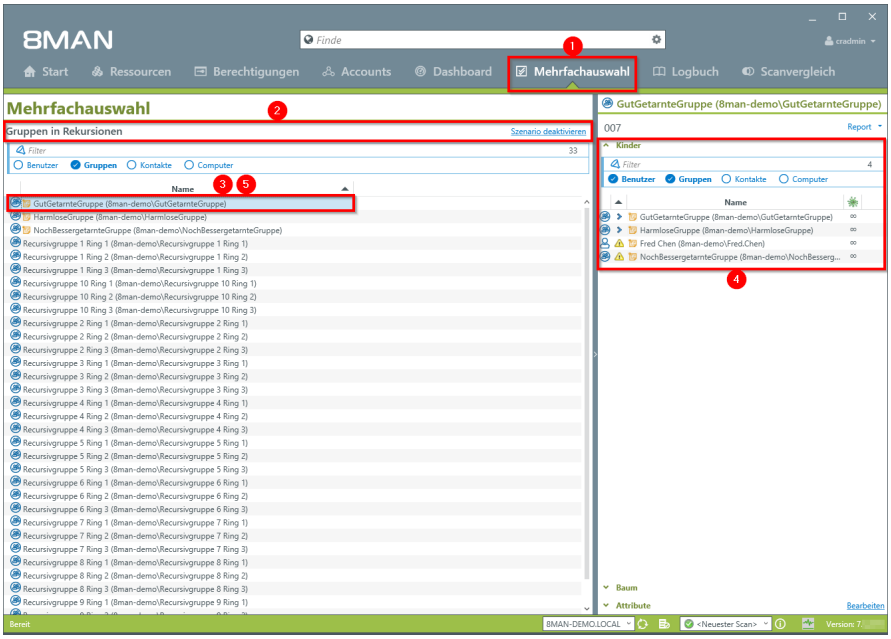
Je höher die Gruppentiefe, desto eher kommt es zu Rekursionen. Behalten Sie deshalb die Verschachtelungstiefe Ihrer Gruppen im Blick.

Gruppen in Rekursion auflisten (Webclient)

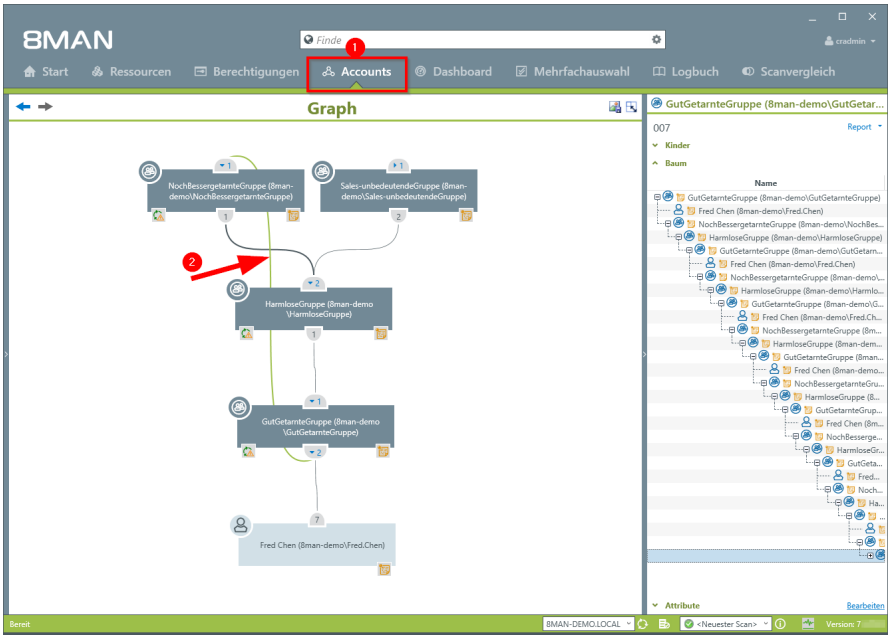
Der Prozess in einzelnen Schritten



1. *Wechseln Sie zum Dashboard.*
2. *Doppelklicken Sie auf "Gruppen in Rekursionen".*



1. *8MAN startet automatisch die Mehrfachauswahl.*
2. *Das Szenario "Gruppen in Rekursion" ist aktiv. 8MAN listet alle Gruppen in Rekursionen auf.*
3. *Klicken Sie auf eine der Gruppen.*
4. *8MAN listet alle Benutzer und Gruppen in der gewählten Rekursion auf.*
5. *Doppelklicken Sie auf eine Gruppe.*



1. *8MAN wechselt in die Accounts-Ansicht. Darin sehen Sie die für das Beispiel erstellte Rekursion über 3 Ebenen.*
2. *Die grüne Linie im Graph indiziert in dem Beispiel die Rekursion.*

4.1.1.8 Gruppen in Rekursion identifizieren (Webclient)

Hintergrund / Mehrwert

Gruppen können Mitglieder von Gruppen sein. Active Directory lässt es zu, dass Kinder auch wieder Eltern im eigenen „Stammbaum“ werden. Schliessen sich die Verschachtelungen im Kreis, entstehen unsinnige Zirkelbezüge.

Durch diese sogenannten Rekursionen erhält jeder Benutzer, der in irgendeiner der verschachtelten Gruppen Mitglied ist, die Rechte aller beteiligten Gruppen. Die Folge ist eine unübersichtliche und schwer zu identifizierende Überberechtigung. 8MAN identifiziert automatisch alle Rekursionen in Ihrem System. Wir empfehlen diese zu unterbrechen.

TIP: Administrieren Sie nur noch mit 8MAN und Rekursionen können nicht mehr entstehen.

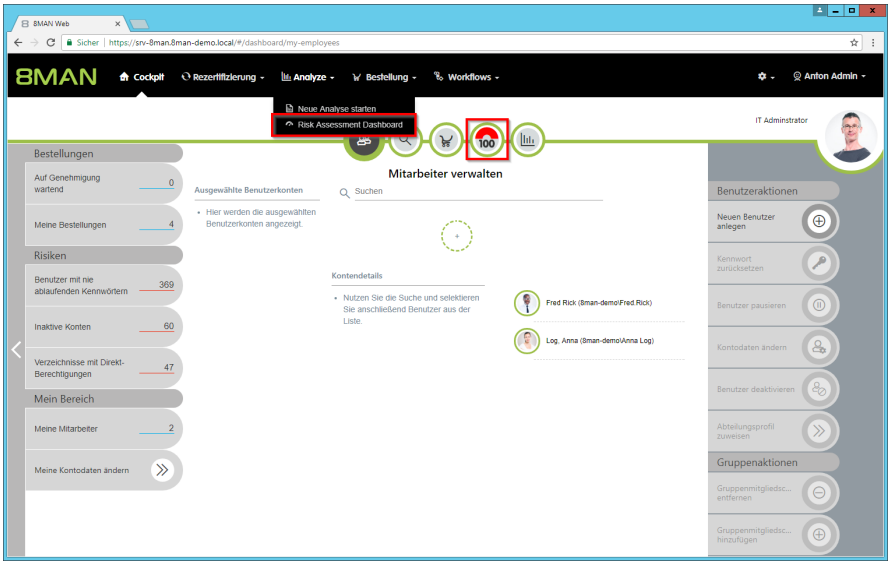
Weiterführende Services

Je höher die Gruppentiefe, desto eher kommt es zu Rekursionen. Behalten Sie deshalb die Verschachtelungstiefe Ihrer Gruppen im Blick.

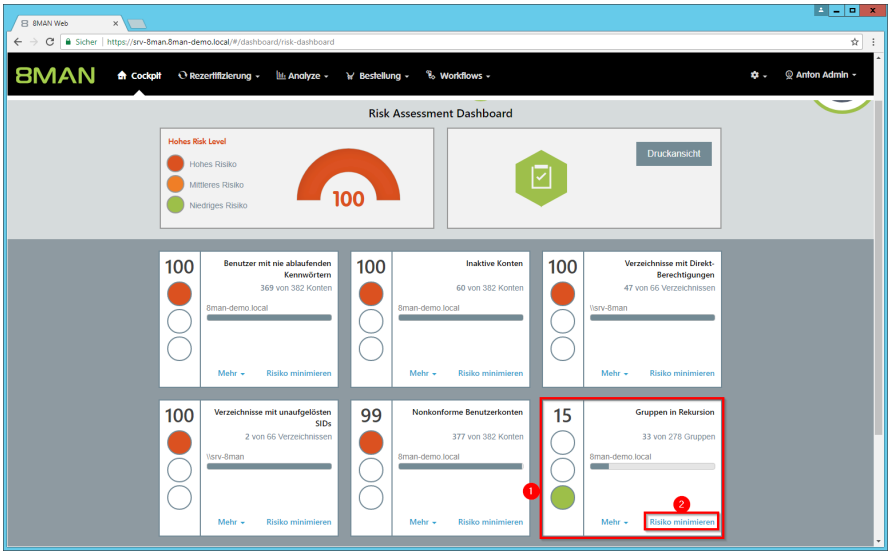
Identifizieren Sie rekursive Gruppen im Rich Client.

Lösen Sie die Rekursion auf, in dem Sie Gruppenmitgliedschaften im Rich Client bearbeiten oder Gruppenmitgliedschaften im Webclient entfernen.

Der Prozess in einzelnen Schritten

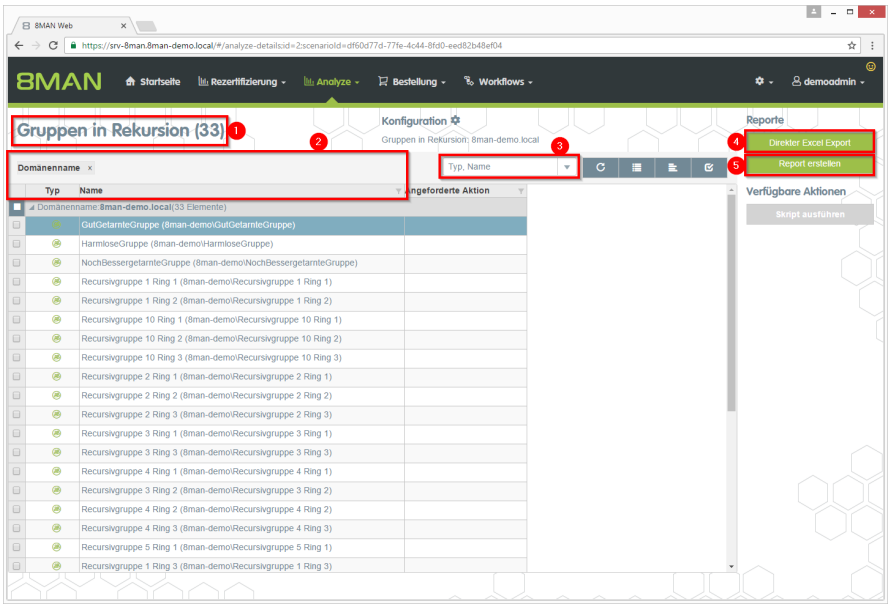


Rufen Sie das Risk Assessment Dashboard auf.



1. *Auf der Kachel "Gruppen in Rekursion" sehen Sie eine Bewertung des Risikofaktors.*
2. *Klicken Sie auf "Risiko minimieren".*

Die Kacheln sind nach Risikobewertung sortiert und können sich deshalb an unterschiedlichen Stellen befinden.



1. *8MAN zeigt Ihnen eine Auflistung aller Gruppen in Rekursion.*
2. *Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen für Ihre Analyse.*
3. *Wählen Sie die angezeigten Spalten aus. Die Auswahl gilt auch für die Reporte.*
4. *Exportieren Sie die angezeigten Daten direkt in das Excel-Format.*
5. *Erstellen Sie einen Report im PDF- oder CSV-Format. Speichern Sie den Report oder versenden ihn per E-Mail.*

4.1.1.9 Benutzer mit nie ablaufenden Kennwörtern identifizieren (Report)

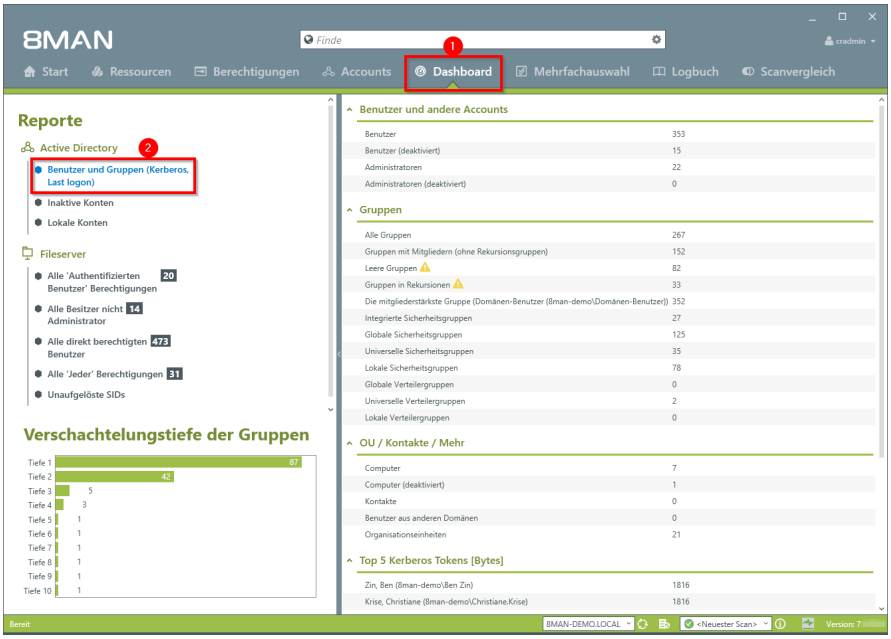
Hintergrund / Mehrwert

Eine zentrale Sicherheitsanforderung im Firmennetzwerk ist die regelmäßige Änderung der Kennwörter. 8MAN durchsucht die Domäne nach Nutzerkonten, bei denen diese Anforderung nicht aktiviert wurde. Die Informationen entnehmen Sie bitte unserem Report "Benutzer und Gruppen".

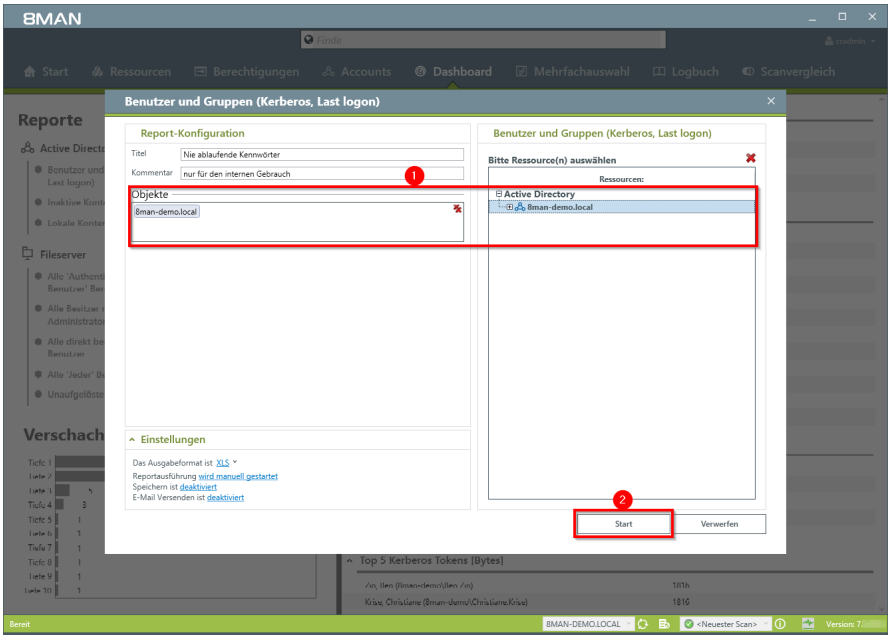
Weiterführende Services

Ein Kennwort zurücksetzen
Kennwortoptionen eines Benutzers ändern
Benutzer mit nie ablaufenden Kennwörtern identifizieren (im Webclient)
Kennwortoptionen im Bulk ändern (im Webclient)

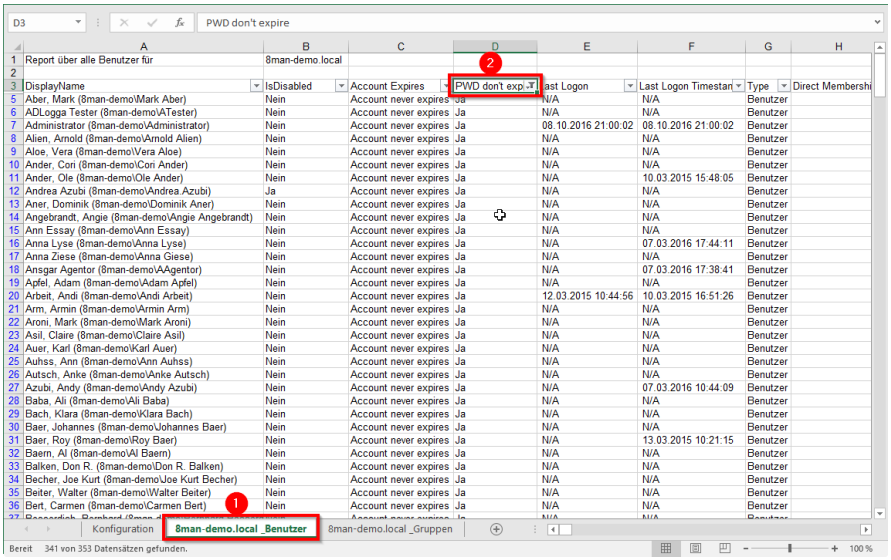
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Dashboard".*
2. *Klicken Sie auf "Benutzer und Gruppen" im Bereich "Reporte".*



1. *Bestimmen Sie den Umfang des Reports mit Drag & Drop.*
2. *Starten Sie die Reporterstellung.*



Öffnen Sie den Report in Excel.

1. *Wechseln Sie in das Tabellenblatt "... _Benutzer"*
2. *Filtern Sie in der Spalte "PWD don't expire" nach positiven Ergebnissen.*

Wir empfehlen, die Sicherheitsrichtlinien für Benutzerkonten so einzustellen, dass Benutzer ihr Kennwort spätestens nach 90 Tagen ändern müssen.

4.1.1.10 Benutzer mit nie ablaufenden Kennwörtern identifizieren (Webclient)

Hintergrund / Mehrwert

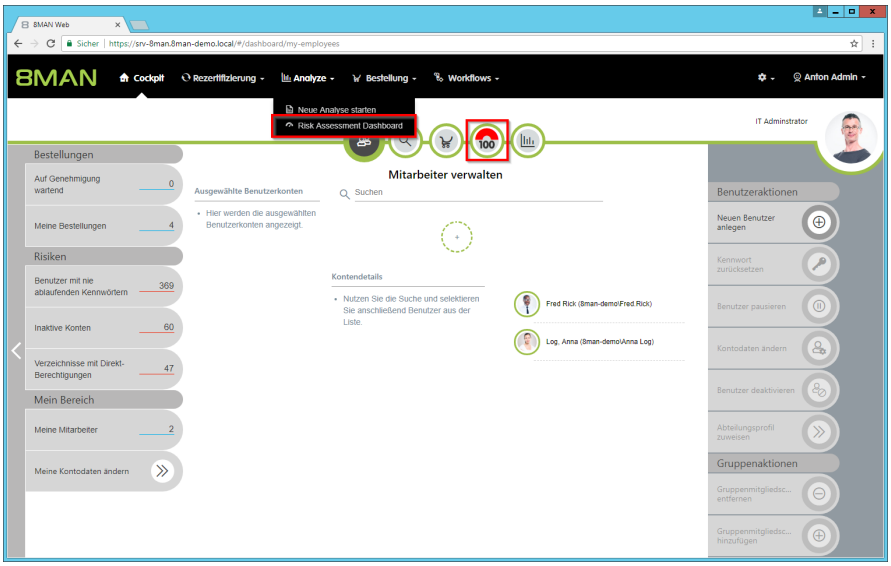
Eine zentrale Sicherheitsanforderung im Firmennetzwerk ist die regelmäßige Änderung der Kennwörter. 8MAN durchsucht die Domäne nach Nutzerkonten, bei denen diese Anforderung nicht aktiviert wurde.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.11 Regelung des Passwortgebrauchs sowie M 4.48 Passwortschutz unter Windows-Systemen.

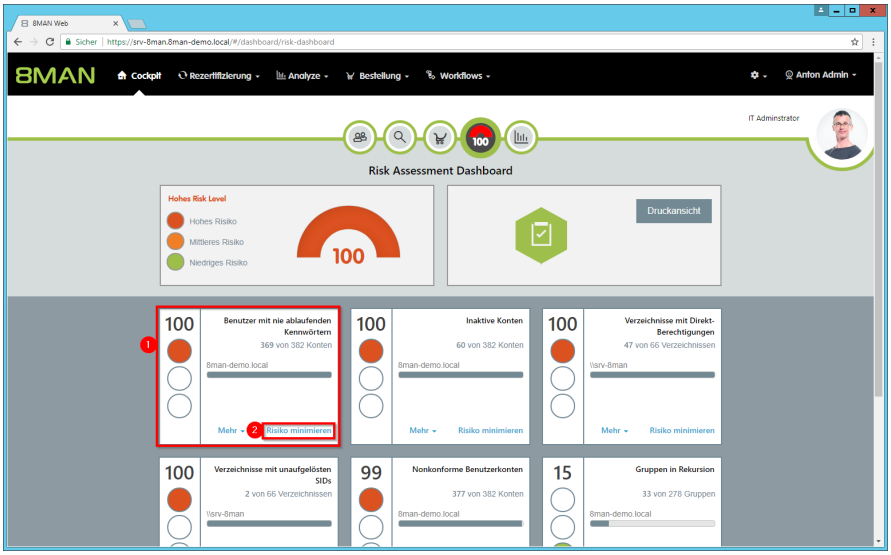
Weiterführende Services

Ein Kennwort zurücksetzen
Kennwortoptionen eines Benutzers ändern

Der Prozess in einzelnen Schritten

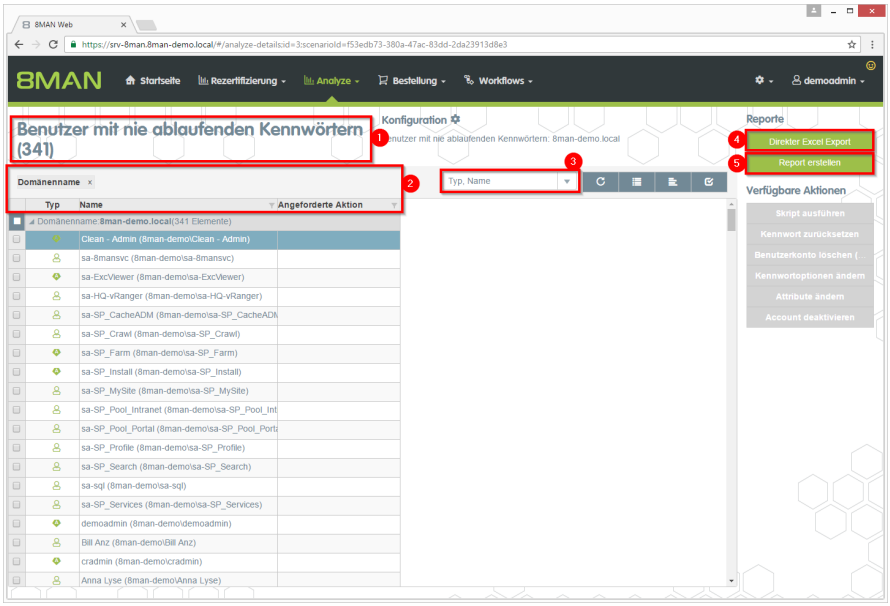


Rufen Sie das Risk Assessment Dashboard auf.



1. *Auf der Kachel "Benutzer mit nie ablaufenden Kennwörtern" sehen Sie eine Bewertung des Risikofaktors.*
2. *Klicken Sie auf "Risiko minimieren".*

Die Kacheln sind nach Risikobewertung sortiert und können sich deshalb an unterschiedlichen Stellen befinden.



1. *8MAN zeigt Ihnen eine Auflistung aller Benutzer mit nie ablaufenden Kennwörtern.*
2. *Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen für Ihre Analyse.*
3. *Wählen Sie die angezeigten Spalten aus. Die Auswahl gilt auch für die Reporte.*
4. *Exportieren Sie die angezeigten Daten direkt in das Excel-Format.*
5. *Erstellen Sie einen Report im PDF- oder CSV-Format. Speichern Sie den Report oder versenden ihn per E-Mail.*

4.1.1.11 Die AD Situation aus der Vergangenheit analysieren

Hintergrund / Mehrwert

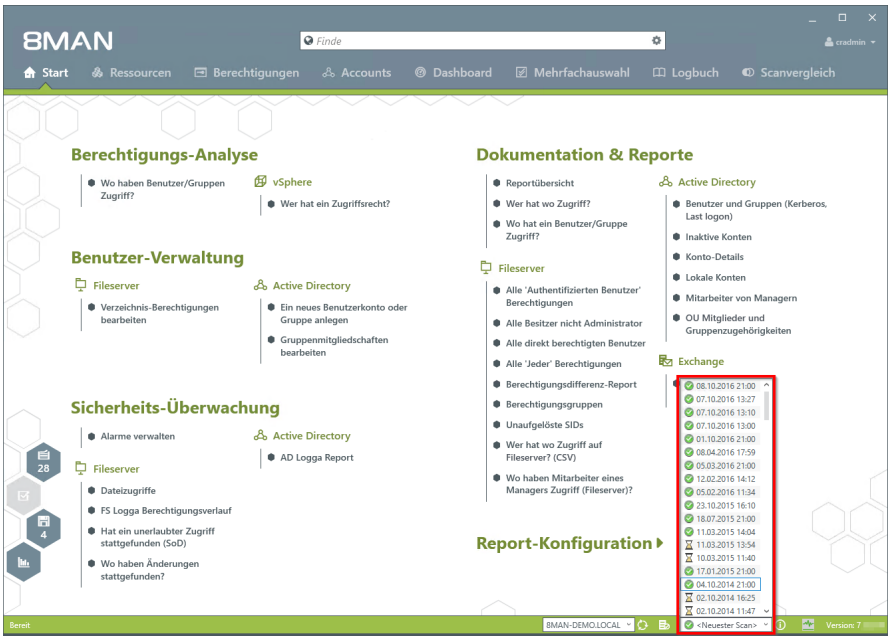
Nach Sicherheitsvorfällen empfielt sich ein Blick auf die Berechtigungssituation aus der Vergangenheit. Wer hatte Zugriff und wer ist aus systemischer Sicht entlastet?

Mit 8MAN können Sie alte Scans abrufen und im gewohnten "Look and Feel" die Situation zum Zeitpunkt der Erhebung im AD nachvollziehen.

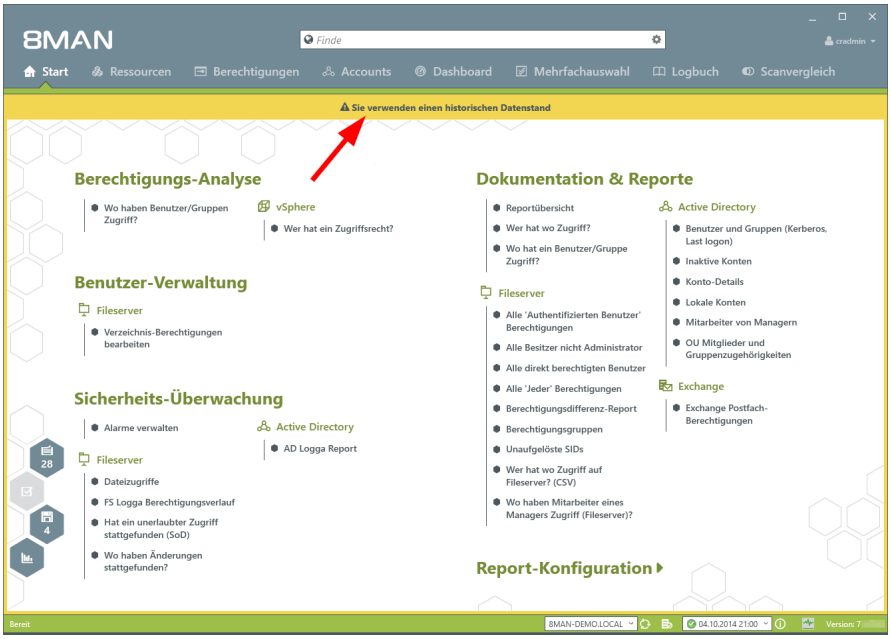
Weiterführende Services

Alternativ können Sie auch zwei Scan Zeitpunkte miteinander vergleichen.

Der Prozess in einzelnen Schritten



Wählen Sie das Scandatum, welches Sie interessiert.



Die Warnmeldung und der orange Rahmen signalisieren, dass Sie sich in der Vergangenheit bewegen.

4.1.1.12 Inaktive Konten identifizieren (Webclient)

Hintergrund / Mehrwert

Inaktive Konten können unerkannt von Menschen oder Schadsoftware für Datendiebstahl und Manipulation genutzt werden. Oft sind Sie ein Indiz für eine gestörte Kommunikation zwischen der Personalabteilung und der IT, denn: Inaktive Nutzerkonten sind oft die Überbleibsel längst ausgeschiedener Mitarbeiter. 8MAN zeigt inaktive Konten, deren letzte Anmeldung länger als 30 Tage zurückliegt, für Sie an.

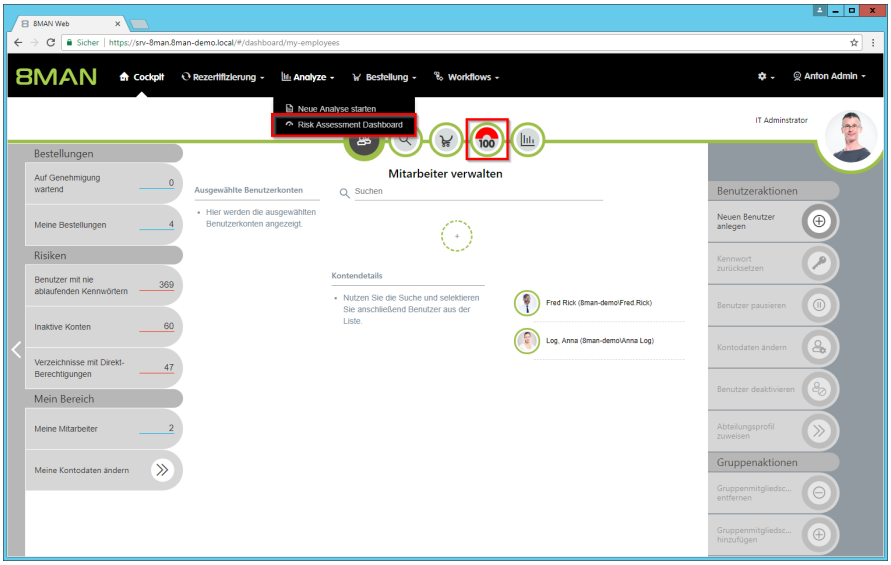
Löschen oder deaktivieren Sie die Konten, die keine Funktion mehr erfüllen.

Weiterführende Services

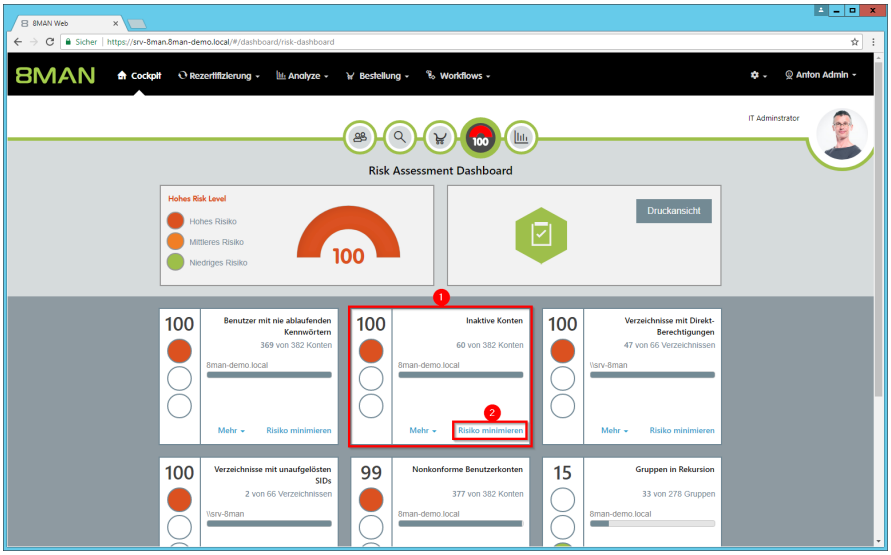
Report: Inaktive Konten finden

Konten im Bulk deaktivieren (Webclient)

Der Prozess in einzelnen Schritten

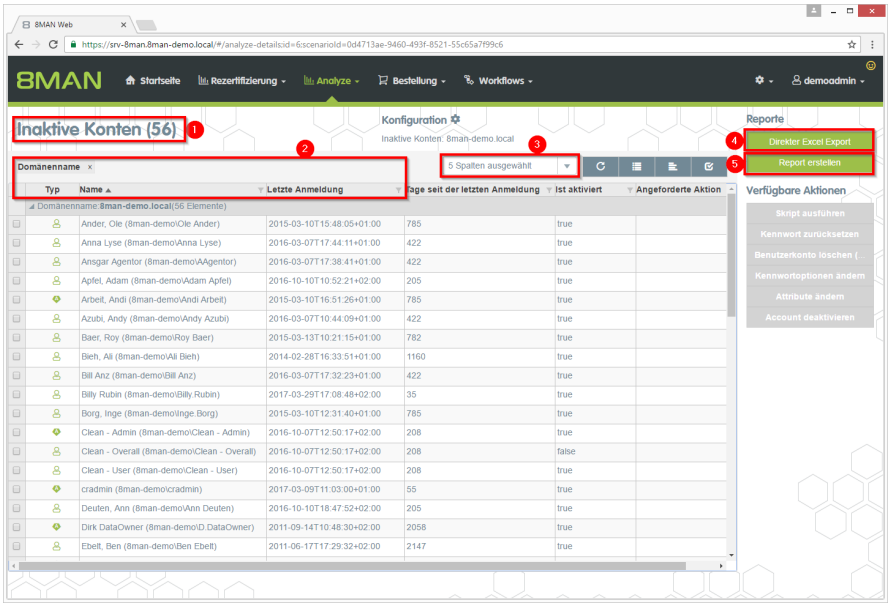


1. *Rufen Sie das Risk Assessment Dashboard auf.*



1. *Auf der Kachel "Inaktive Konten" sehen Sie eine Bewertung des Risikofaktors.*
2. *Klicken Sie auf "Risiko minimieren".*

Die Kacheln sind nach Risikobewertung sortiert und können sich deshalb an unterschiedlichen Stellen befinden.



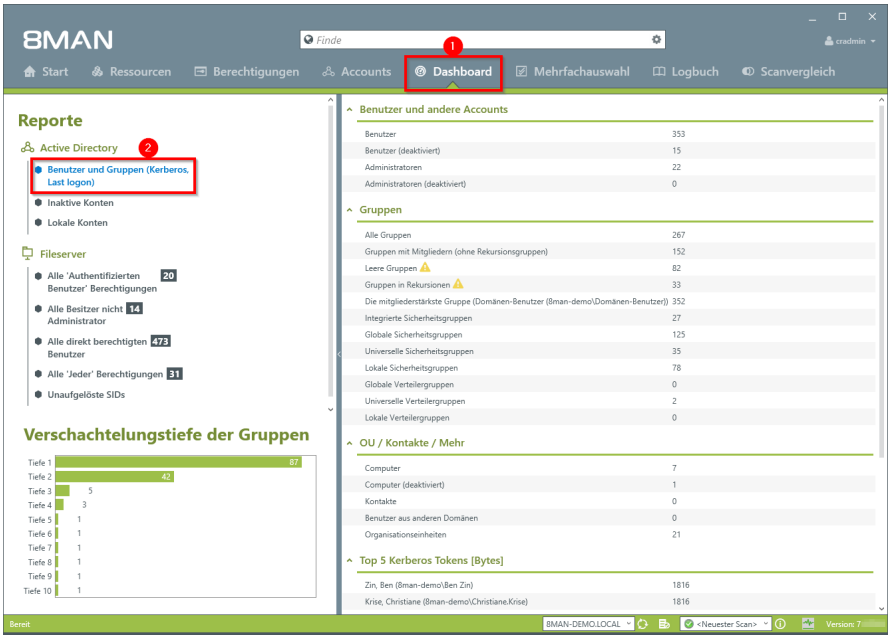
1. *8MAN zeigt Ihnen eine Auflistung aller inaktiven Konten.*
2. *Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen für Ihre Analyse.*
3. *Wählen Sie die angezeigten Spalten aus. Die Auswahl gilt auch für die Reporte.*
4. *Exportieren Sie die angezeigten Daten direkt in das Excel-Format.*
5. *Erstellen Sie einen Report im PDF- oder CSV-Format. Speichern Sie den Report oder versenden ihn per E-Mail.*

4.1.1.13 Temporäre Nutzerkonten identifizieren

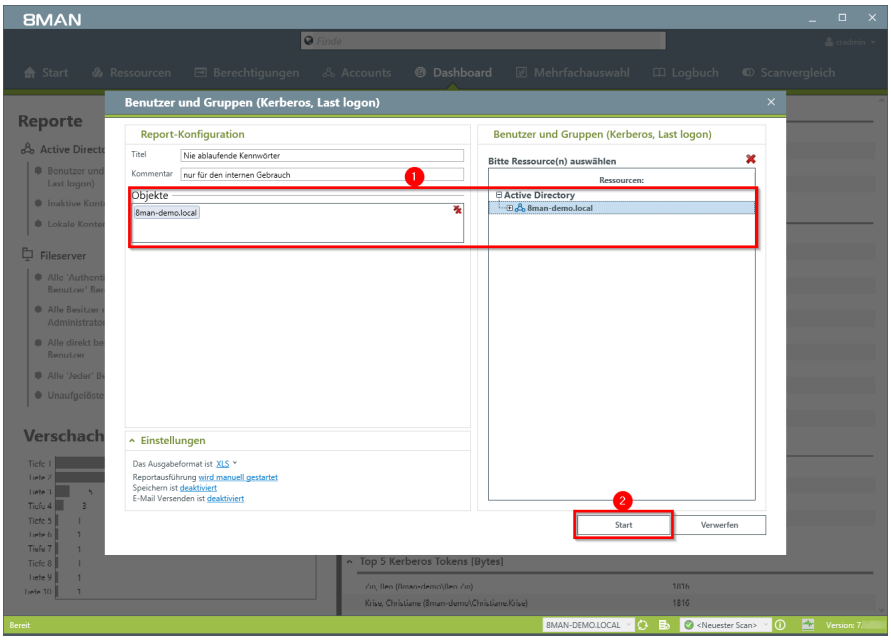
Hintergrund / Mehrwert

Nutzerkonten von Beratern oder Auszubildenden sollten nur temporär angelegt werden. Mit 8MAN behalten Sie den Überblick über temporäre Nutzerkonten. Die Informationen dazu entnehmen Sie bitte dem Report "Benutzer und Gruppen".

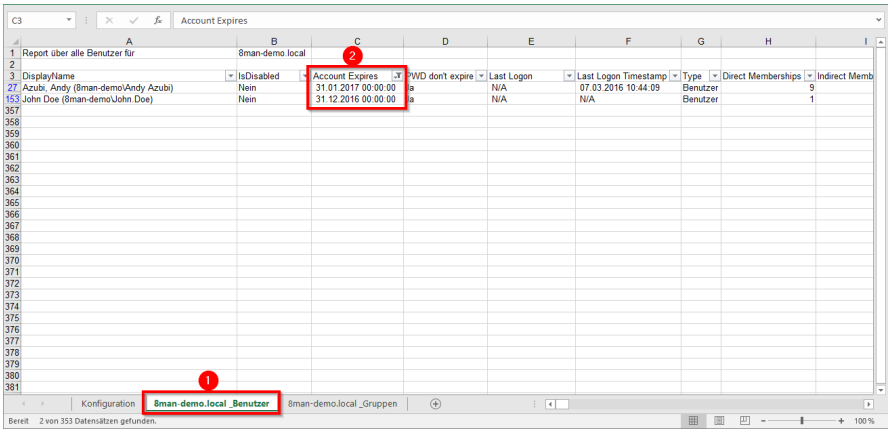
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Dashboard".*
2. *Klicken Sie auf "Benutzer und Gruppen" im Bereich "Reporte".*



1. *Bestimmen Sie den Umfang des Reports mit Drag & Drop.*
2. *Starten Sie die Reporterstellung.*



Öffnen Sie den Report in Excel.

1. *Wechseln Sie in das Tabellenblatt "... _Benutzer"*
2. *Filtern Sie in der Spalte "Account Expires" nach positiven Ergebnissen.*

Wir empfehlen, in Zusammenarbeit mit der Personalabteilung temporäre Mitarbeiter zu identifizieren und zu prüfen, ob die Konten noch gebraucht werden.

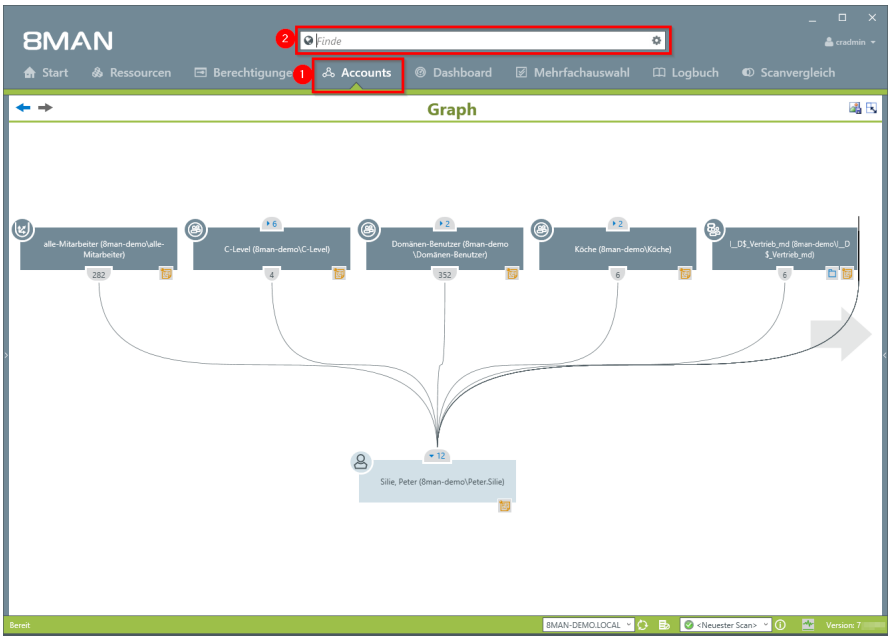
4.1.1.14 Die letzten Aktionen an einem Account identifizieren

Hintergrund / Mehrwert

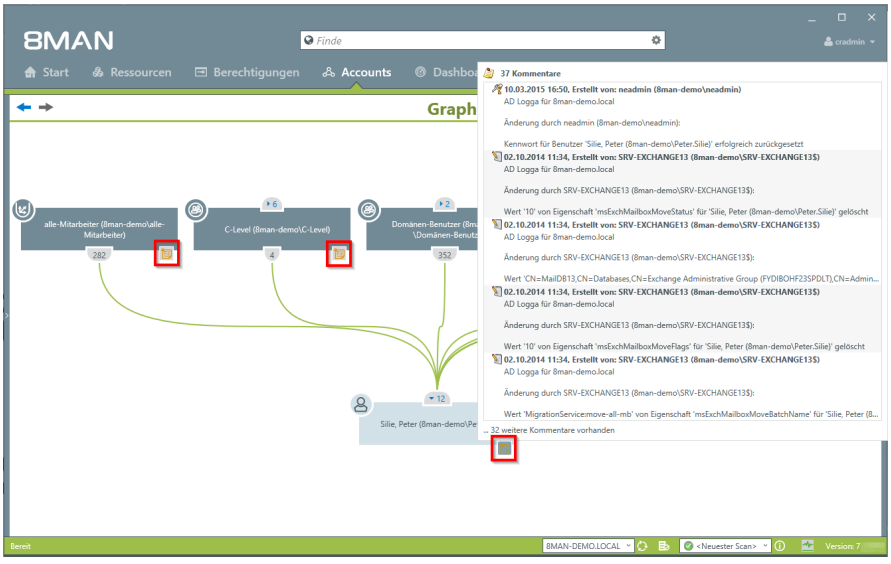
Nutzerkonten und Gruppen haben eine eigene Historie. Deshalb macht es Sinn, vor der weiteren Bearbeitung zu prüfen, was vorher durchgeführte Aktivitäten waren.

8MAN zeigt in einer Schnellansicht die letzten Aktivitäten oder Sie gelangen direkt in das Logbuch, um eine vollständige Auflistung zu erhalten.

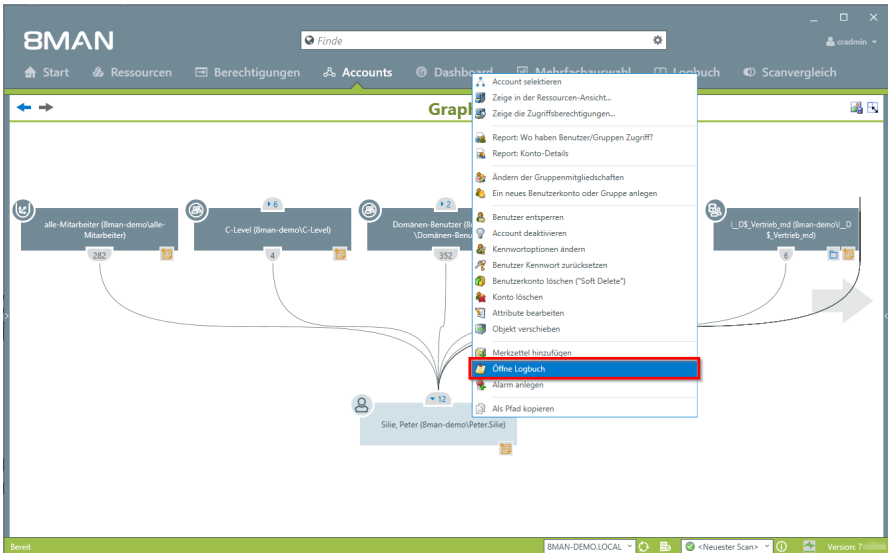
Der Prozess in einzelnen Schritten



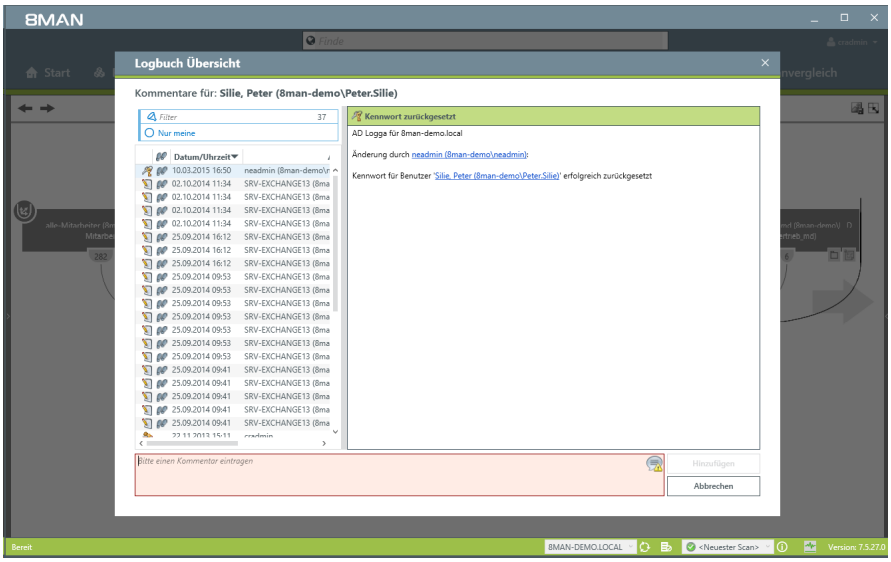
1. *Wählen Sie "Accounts".*
2. *Suchen Sie nach dem gewünschten Nutzer oder der gewünschten Gruppe.*



An dem Notizzettel-Symbol erkennen Sie, dass Aktivitäten im 8MAN Logbuch aufgezeichnet sind. Fahren Sie mit dem Mauszeiger über das Symbol, um eine Kurzübersicht der letzten Aktivitäten zu erhalten, die an dem Account durchgeführt wurden.



Klicken Sie mit rechts auf das gewünschte Objekt und wählen dann "Öffne Logbuch", um alle aufgezeichneten Informationen zu erhalten.



Prüfen Sie die am Objekt bereits durchgeführten Aktivitäten. Sie können einen Kommentar in das Logbuch schreiben. An dem "Fußspuren-Symbol" erkennen Sie, dass die Ereignisse vom AD Logga aufgezeichnet wurden.

4.1.1.15 Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check) (Webclient)

Hintergrund / Mehrwert

8MAN setzt im Bereich User Provisioning neue Maßstäbe: Mit der Einführung von Abteilungsprofilen definieren Abteilungsleiter zusammen mit der Geschäftsführung und dem Compliance Officer den Handlungsradius von Mitarbeitern im Unternehmen.

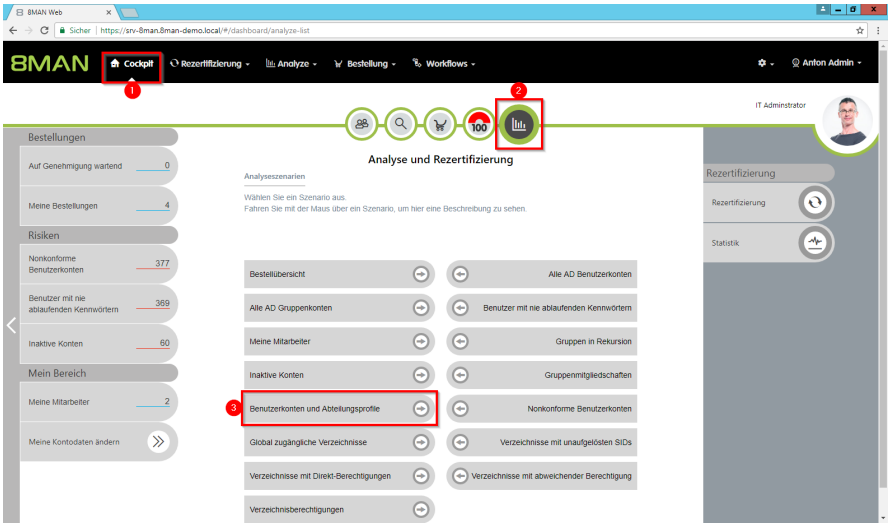
Erhält der Mitarbeiter weitere Berechtigungen, die vom Standard abweichen, zeigt ein Compliance-Monitor dem Vorgesetzten die abweichenden Rechte. In Form von Bulk-Operationen, kann der Abteilungsleiter die Nutzerkonten entsprechend der Profile in seiner Abteilung harmonisieren.

Um die Compliance-Funktionen nutzen zu können, müssen Sie mindestens ein Abteilungsprofil erstellt haben.

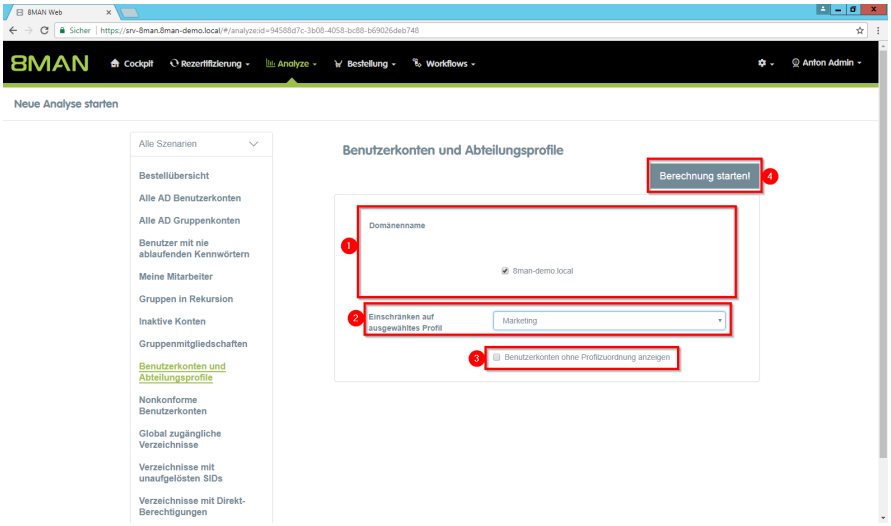
Weiterführende Services

Ein neues Abteilungsprofil erstellen (Administrator)
Benutzern ein Abteilungsprofil zuweisen

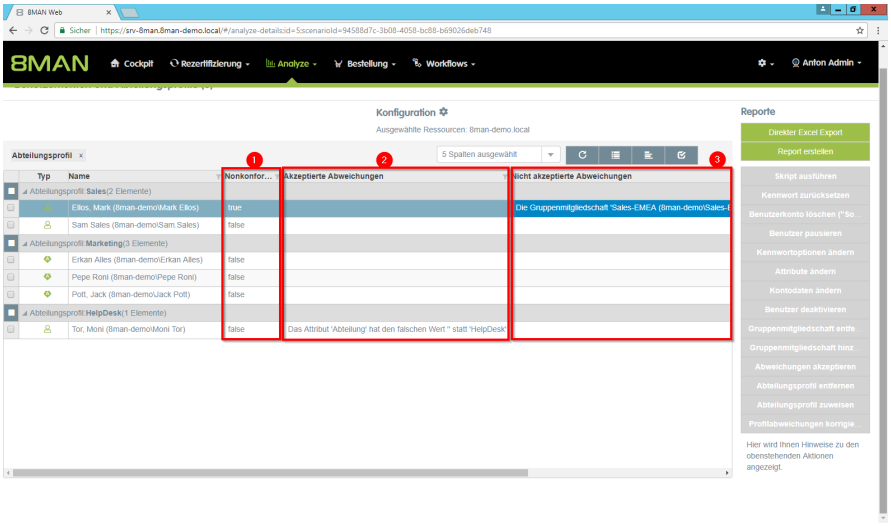
Der Prozess in einzelnen Schritten



1. *Wählen Sie Cockpit.*
2. *Klicken Sie auf "Analyse und Rezertifizierung".*
3. *Klicken Sie auf "Benutzerkonten und Abteilungsprofile".*



1. *Legen Sie fest, welche Domänen in Ihrer Analyse enthalten sind.*
2. *Wählen Sie ein Abteilungsprofil oder alle ("ohne Einschränkung").*
3. *Optional: Aktivieren Sie die Option, wenn auch Benutzer ohne zugewiesenes Abteilungsprofil aufgelistet werden sollen.*



1. *8MAN zeigt Ihnen, welche Benutzerkonten nonkonform sind.*
2. *Benutzerkonten sind konform, wenn Abweichungen von einem Verantwortlichen akzeptiert wurden.*
3. *Benutzerkonten sind nonkonform, wenn "nicht akzeptierte Abweichungen" vorhanden sind.*

4.2 Fileserver

8MAN zeigt alle Berechtigungen auf Fileserverzeichnisse. Administratoren und Data Owner ändern die Berechtigungen in einfachen Workflows. Darüber hinaus zeigt 8MAN Berechtigungsfehler wie Direkt- und Mehrfachberechtigungen, defekte ACLs und unaufgelöste SIDs.

4.2.1 Services für Administratoren und Data Owners

4.2.1.1 Ein Verzeichnis und die Berechtigungen darauf identifizieren

Hintergrund / Mehrwert

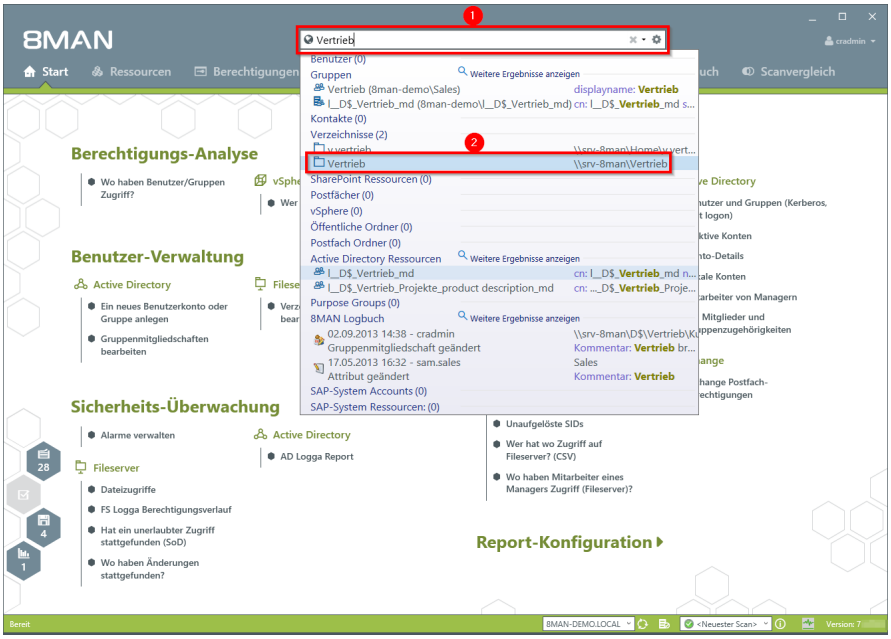
8MAN zeigt Ihnen schnell die vollständige Berechtigungssituation von Fileserververzeichnissen. Prüfen Sie im ersten Schritt die besonders schützenswerten Verzeichnisse. Sie müssen wissen: Wer hat Zugriff?

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.8 Vergabe von Zugriffsrechten.

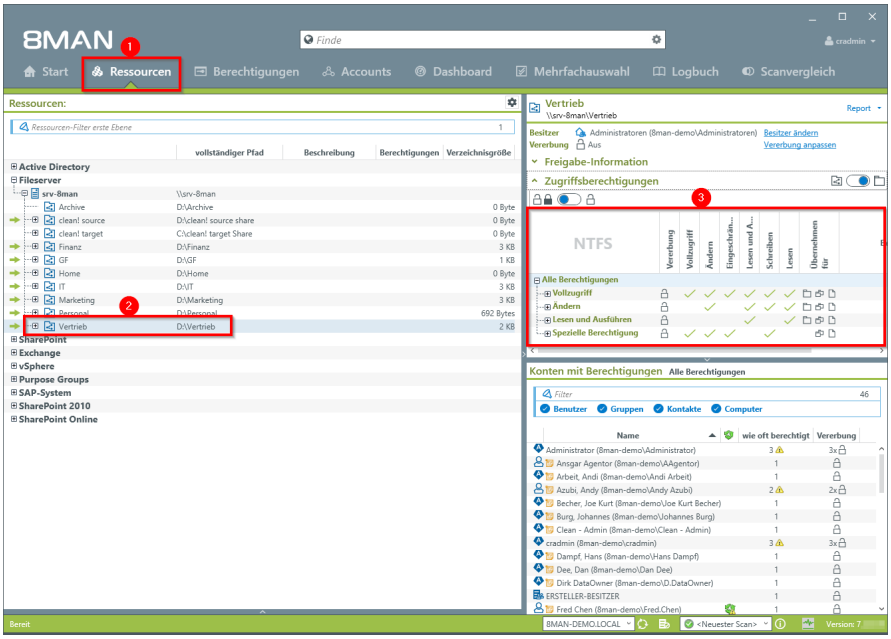
Weiterführende Services

Report: Wer hat wo Zugriff?
Verzeichnis-Berechtigungen ändern.
Die Zugriffe auf das Verzeichnis überwachen

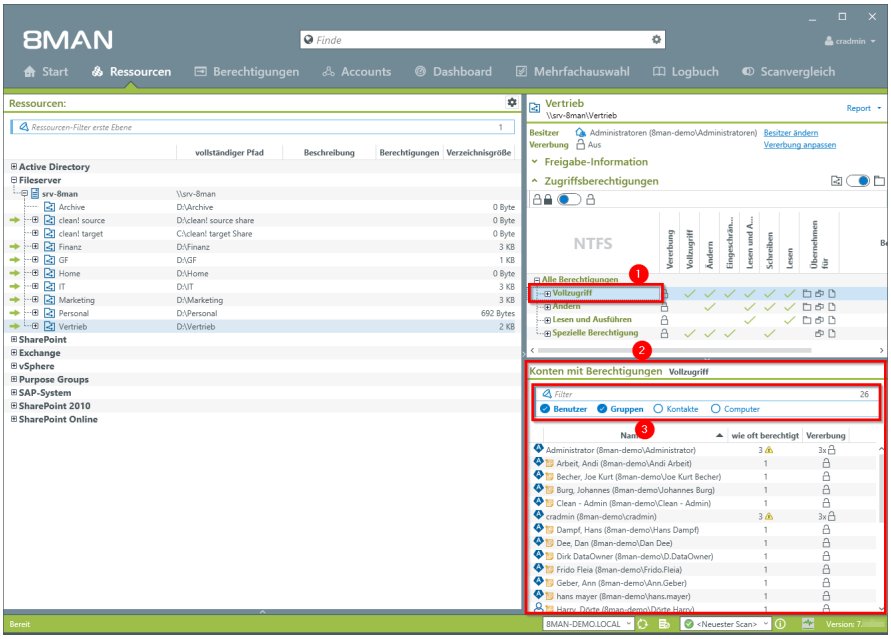
Der Prozess in einzelnen Schritten



1. *Suchen Sie nach dem gewünschten Verzeichnisnamen.*
2. *Sie finden Ihr Suchergebnis im Bereich Verzeichnisse. Klicken Sie auf das Suchergebnis.*



1. *8MAN wechselt in die Ressourcenansicht.*
2. *Sie haben das gesuchte Verzeichnis im Fokus.*
3. *8MAN zeigt Ihnen alle Zugriffsberechtigungen, die für dieses Verzeichnis existieren.*



1. *Wählen Sie oben rechts eine Zugriffskategorie, nach der Sie filtern wollen. Im Beispiel ist "Vollzugriff" selektiert.*
2. *8MAN listet die Konten mit "Vollzugriff" auf das Verzeichnis "Vertrieb" auf.*
3. *Darüber hinaus können Sie die Liste weiter ausdifferenzieren, indem Sie den Filter für Benutzer, Gruppen, Kontakte und Computer (de-)aktivieren.*

4.2.1.2 Die Berechtigungen eines Benutzers identifizieren

Hintergrund / Mehrwert

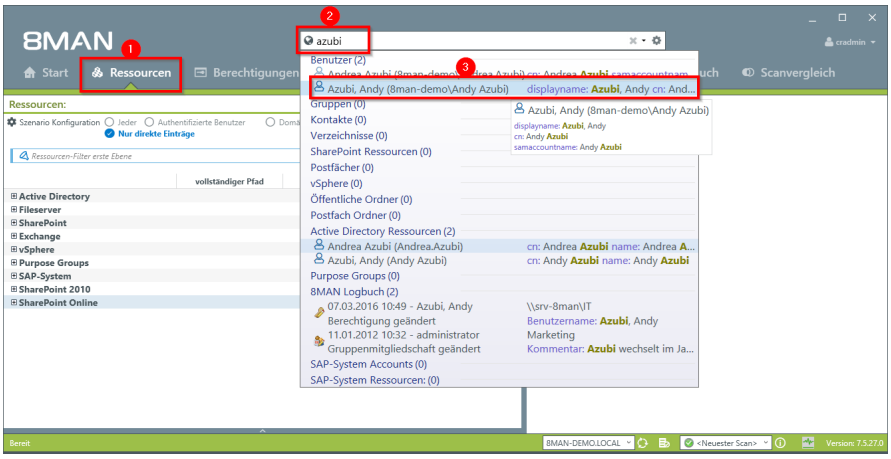
8MAN zeigt auch ausgehend von einzelnen Benutzern, auf welche Ressourcen diese berechtigt sind. Dies ist wichtig, um zu prüfen inwieweit die Rechtesituation zur Rolle des Mitarbeiters passt. Auch hier gilt das "Least Privilege Prinzip". Mitarbeiter, die häufig die Abteilung gewechselt haben, verfügen oftmals über Berechtigungen, die nach der Versetzung wieder entfernt werden können.

Weiterführende Services

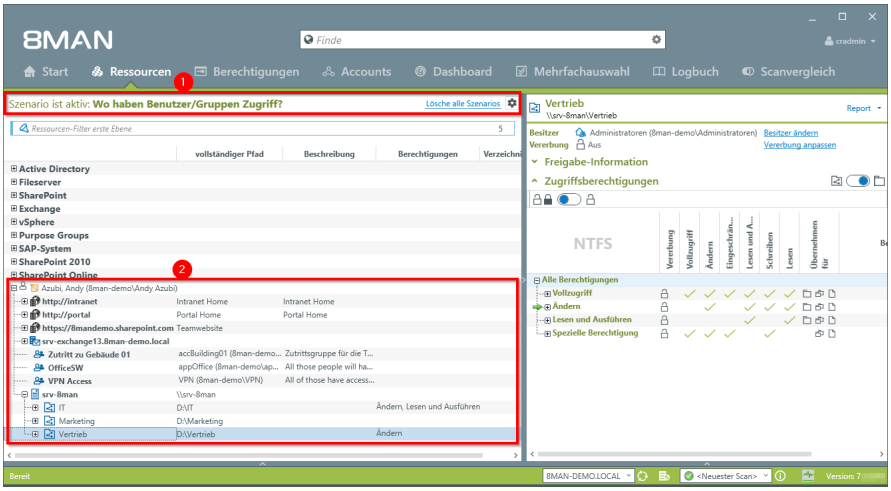
Alternativ können Sie die gleichen Informationen auch in einem Report erfassen: Wo hat ein Benutzer / Gruppen Zugriff?

Im Gegensatz zur dynamischen Ansicht in der UI zeigt der Report keine Informationen zu Active Directory, Exchange und Purpose Groups.

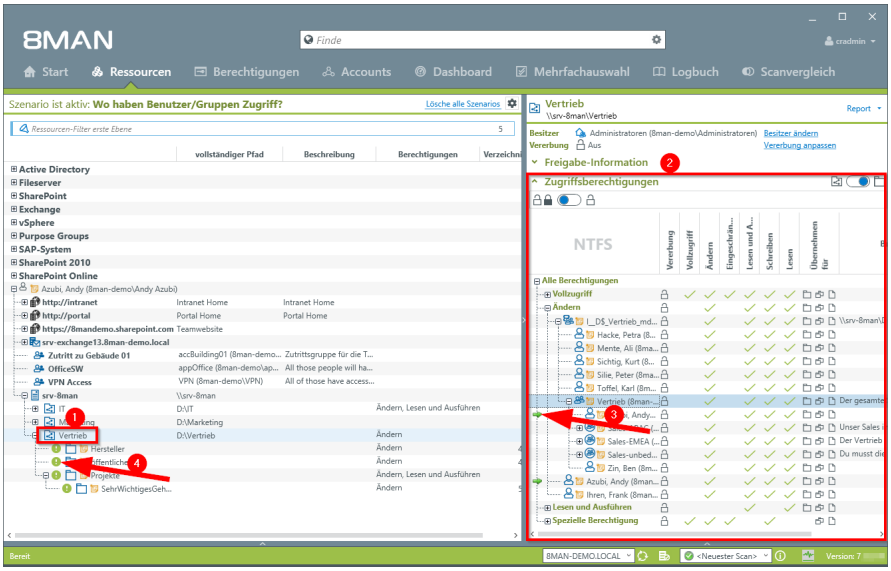
Der Prozess in einzelnen Schritten



1. *Wählen Sie die "Ressourcen".*
2. *Geben Sie den Namen der Person ein, deren Berechtigungssituation sie analysieren möchten.*
3. *Klicken Sie auf das Suchergebnis im Bereich "Benutzer".*



1. *8MAN aktiviert das Szenario "Wo haben Benutzer/Gruppen Zugriff?".*
2. *8MAN zeigt alle Ressourcen, auf die "Andy Azubi" Zugriff hat. In der Basisversion sind Active Directory und Fileserver Berechtigungen abrufbar. Je nachdem welche Add-Ons Sie integriert haben, können Sie weitere Berechtigungen prüfen.*



1. *Im Fileserver-Bereich zeigt 8MAN alle Verzeichnisse, auf die "Andy Azubi" Zugriff hat. In dem Beispiel hier haben wir das Verzeichnis "Vertrieb" im Fokus.*
2. *8MAN zeigt für den Ordner "Vertrieb" die Zugriffsberechtigungen.*
3. *Der grüne Pfeil weist zum gewählten Benutzer "Andy Azubi". So identifizieren Sie, über welche Pfade welche Art von Zugriff "Andy Azubi" hat.*
4. *Der grüne Kreis mit dem Ausrufezeichen zeigt an, dass auf diesen Verzeichnissen die Berechtigungen vom übergeordneten Verzeichnis abweichen.*

4.2.2 Services für Administratoren

4.2.2.1 Mehrfachberechtigungen auf Verzeichnissen identifizieren

Hintergrund / Mehrwert

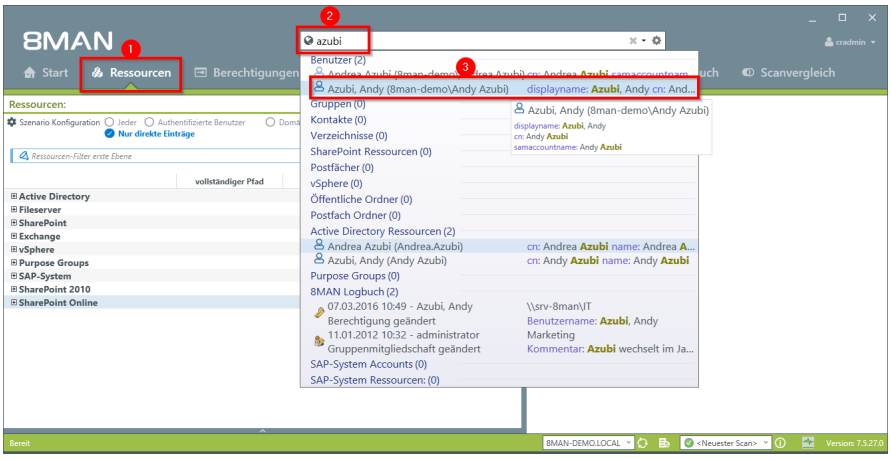
Mehrfachberechtigungen sind Folge von unsauberen Gruppenstrukturen und Direktberechtigungen. Eine Berechtigung sollte sich nur aus einer Gruppenmitgliedschaft ergeben.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.8 Vergabe von Zugriffsrechten.

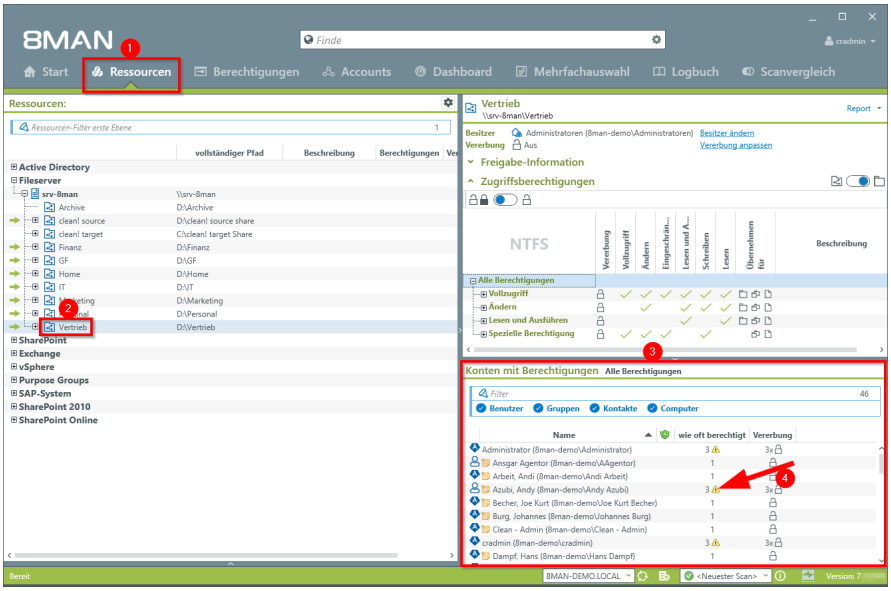
Weiterführende Services

Mehrfachberechtigungen auf Verzeichnissen entfernen

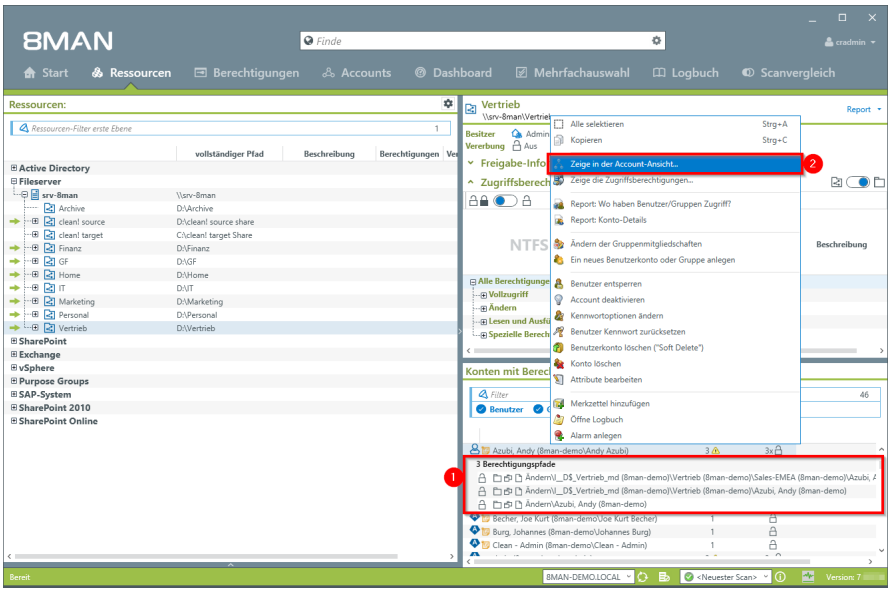
Der Prozess in einzelnen Schritten



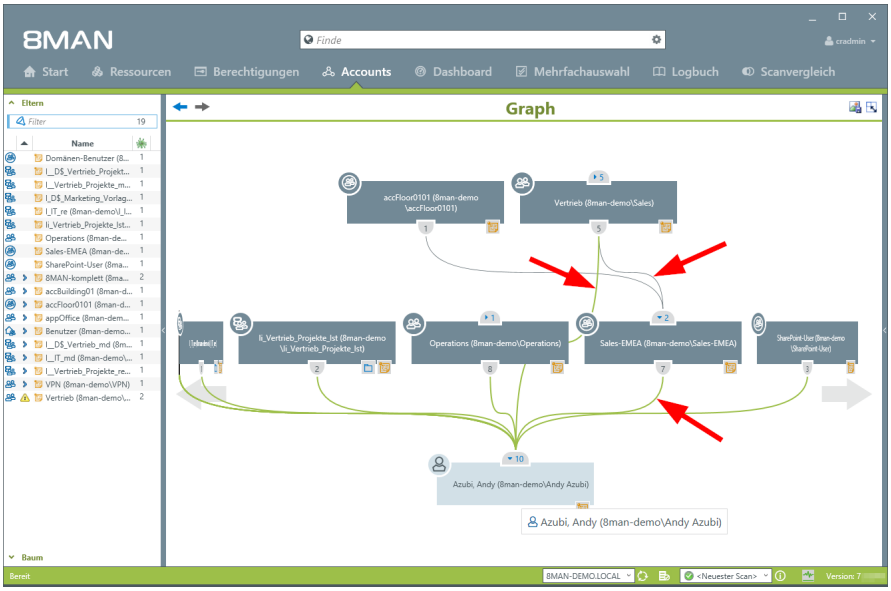
1. *Wählen Sie die "Ressourcen".*
2. *Geben Sie den Namen der Person ein, deren Berechtigungssituation sie analysieren möchten.*
3. *Klicken Sie auf das Suchergebnis im Bereich "Benutzer".*



1. *Wählen Sie "Ressourcen".*
2. *Selektieren Sie ein Verzeichnis.*
3. *8MAN zeigt für alle Berechtigungen in einer flachen Liste die jeweiligen Nutzer.*
4. *Das gelbe Warnsymbol weist Sie auf Mehrfachberechtigungen hin. Klicken Sie darauf.*



1. *8MAN zeigt die verschiedenen Berechtigungspfade (im Beispiel drei) über die "Andy Azubi" den Zugriff auf das Vertriebsverzeichnis erhält.*
2. *Klicken Sie auf den Nutzer mit der rechten Maustaste, um in das Kontextmenü zu gelangen. Wählen Sie "Zeige in der Account-Ansicht...".*



Analysieren Sie mit dem Account-Graphen, wie die Mehrfachberechtigungen aufgebaut sind.

4.2.2.2 Global zugängliche Verzeichnisse identifizieren (Webclient)

Hintergrund / Mehrwert

Werden "Jeder-Konten" für die Vergabe von Berechtigungen benutzt, hat (fast) jeder Zugriff auf verknüpfte Ressourcen.
Die Folge ist eine massive Überberechtigung, also eine hohe Chance für unberechtigte Zugriffe.
Zu den "Jeder-Konten" gehören:

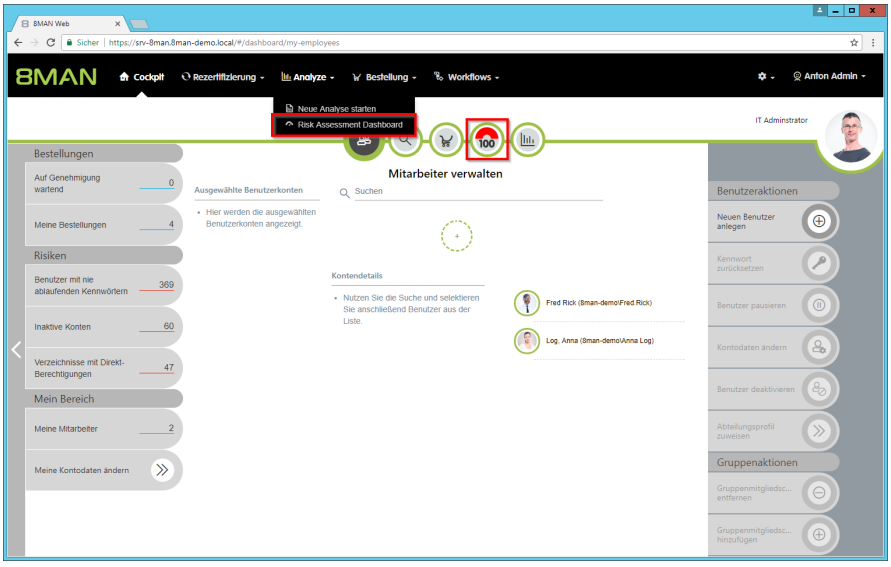
- Jeder
- Authentifizierte Benutzer
- Domänen-Benutzer

Bevor Sie die Berechtigungen löschen, sollten Sie die entsprechenden Ressourcen bestimmen und diesen spezifische Gruppen zuweisen.

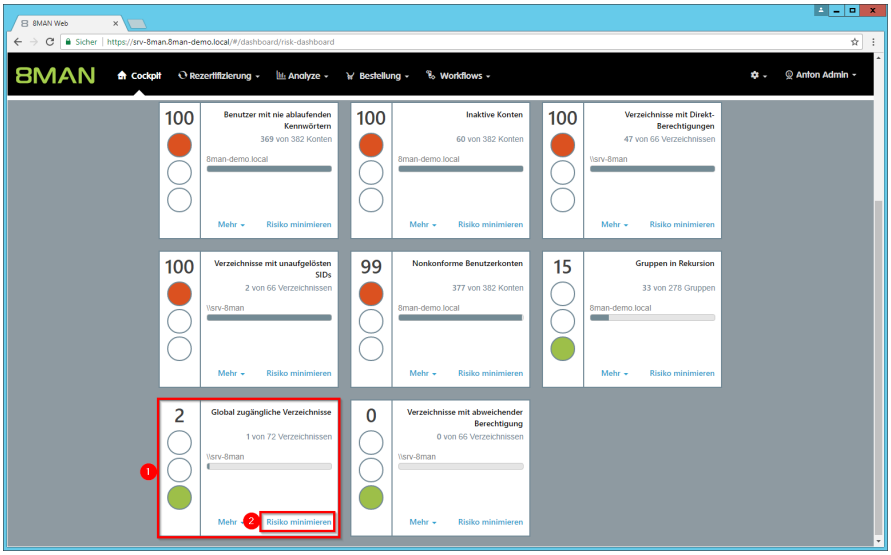
Weiterführende Services

Jeder Berechtigungen im Bulk entfernen

Der Prozess in einzelnen Schritten

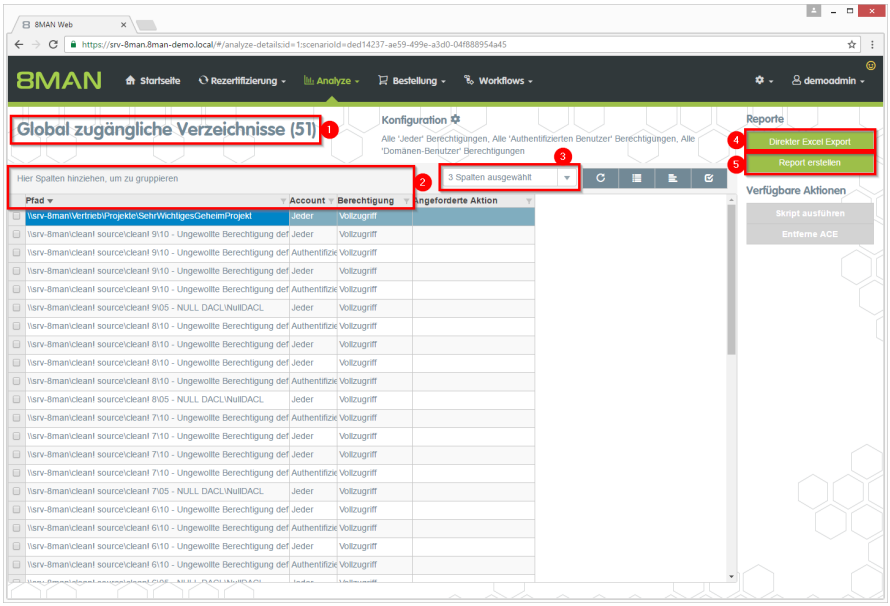


Rufen Sie das Risk Assessment Dashboard auf.



1. *Auf der Kachel "Global zugängliche Verzeichnisse" sehen Sie eine Bewertung des Risikofaktors.*
2. *Klicken Sie auf "Risiko minimieren".*

Die Kacheln sind nach Risikobewertung sortiert und können sich deshalb an unterschiedlichen Stellen befinden.



1. *8MAN zeigt Ihnen eine Auflistung aller global zugänglichen Verzeichnisse.*
2. *Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen für Ihre Analyse.*
3. *Wählen Sie die angezeigten Spalten aus. Die Auswahl gilt auch für die Reporte.*
4. *Exportieren Sie die angezeigten Daten direkt in das Excel-Format.*
5. *Erstellen Sie einen Report im PDF- oder CSV-Format. Speichern Sie den Report oder versenden ihn per E-Mail.*

4.2.2.3 Vererbungsfehler identifizieren

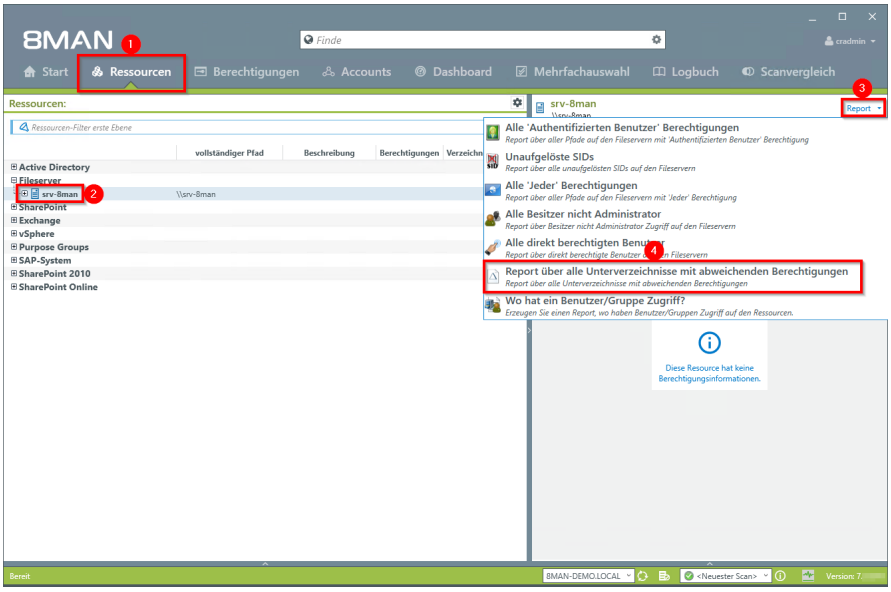
Hintergrund / Mehrwert

Gebrochene ACL's (Access Control Lists) stören die NTFS-Vererbung auf dem Fileserver. Die Folgen: Das Unterverzeichnis erhält nicht die korrekt vererbten Berechtigungen, obwohl die Vererbung aktiviert ist. 8MAN zeigt Ihnen defekte ACLs in einem Report.

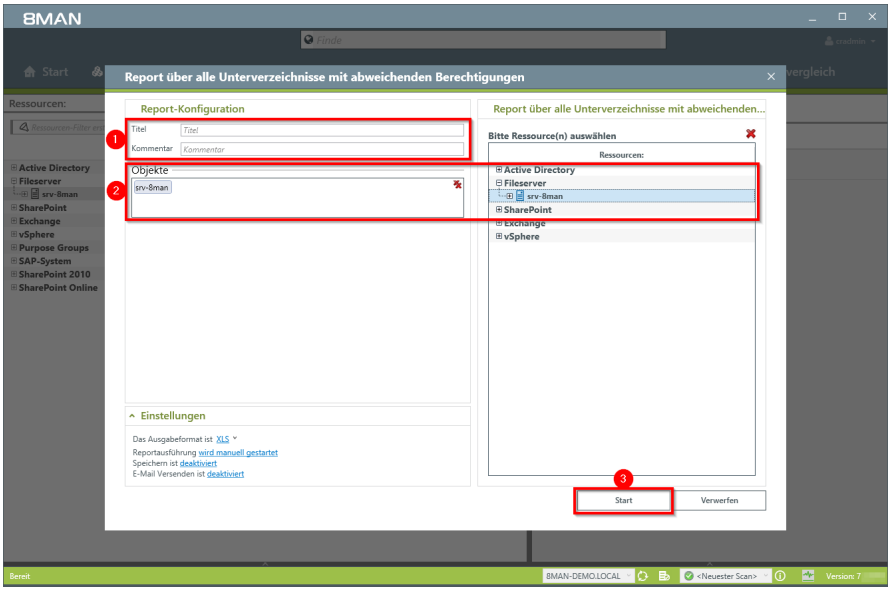
Weiterführende Services

Broken ACLs identifizieren und mit Hilfe der Vererbung korrigieren

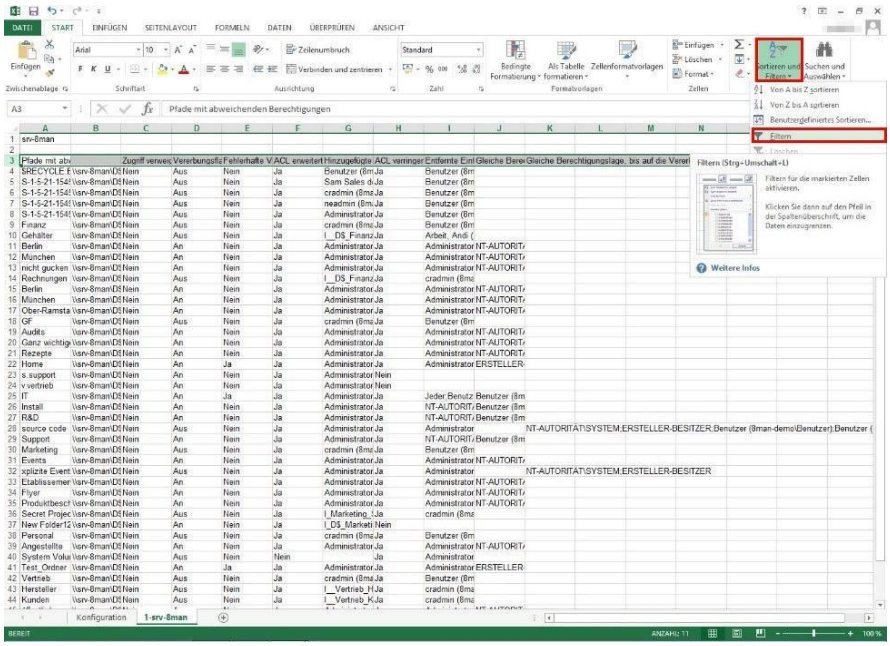
Der Prozess in einzelnen Schritten



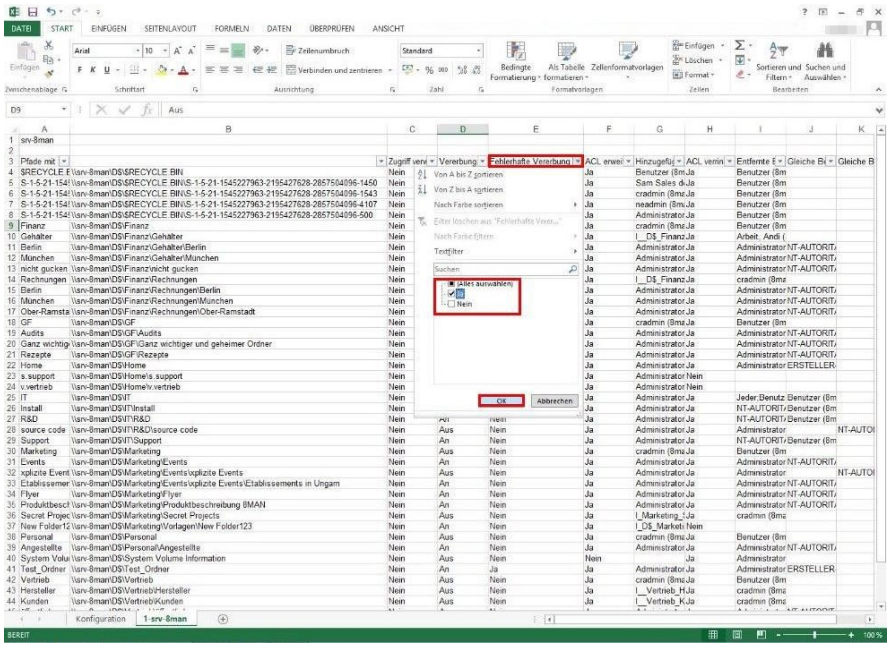
1. *Wählen Sie "Ressourcen".*
2. *Wählen Sie den gewünschten Fileserver.*
3. *Klicken Sie auf "Report".*
4. *Wählen Sie den "Report über alle Unterverzeichnisse mit abweichenden Berechtigungen".*



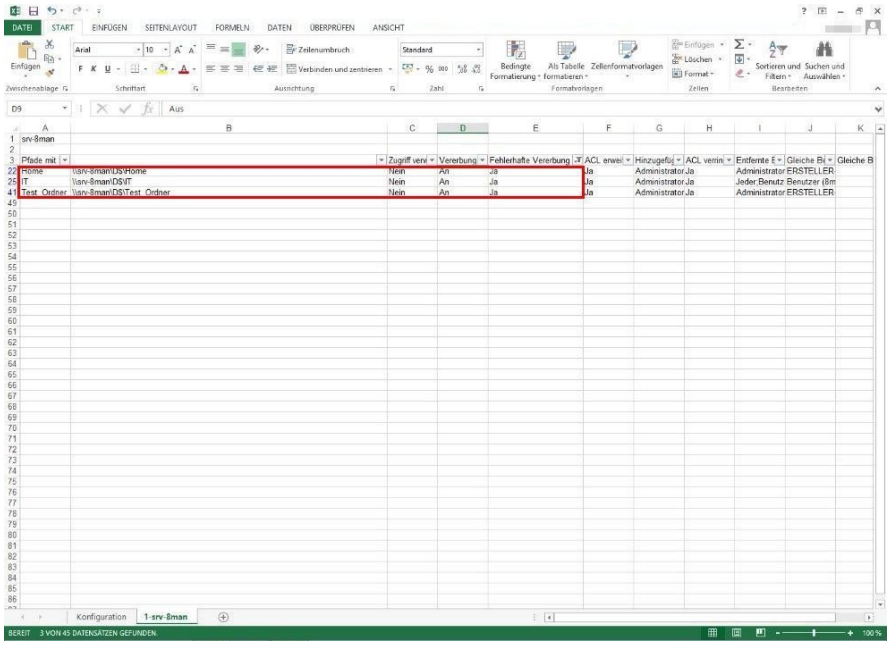
1. *Sie können dem Report einen Namen geben und einen Kommentar hinzufügen.*
2. *Ändern Sie ggf. den Umfang des Reports.*
3. *Starten Sie die Reporterstellung.*



Öffnen Sie die XLS-Datei mit Excel. Markieren Sie die oberste Zeile und fügen einen Filter ein.



Aktivieren Sie in der Spalte "Fehlerhafte Vererbung" die Checkbox "Ja". Klicken Sie auf "OK".



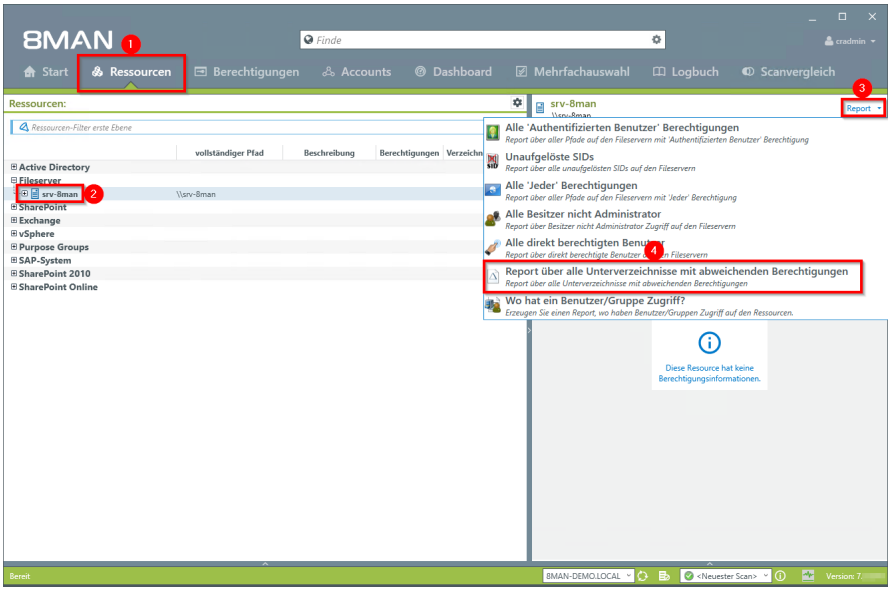
Im Ergebnis erhalten Sie die Verzeichnisse, deren ACLs defekt sind.

4.2.2.4 Besonders geschützte Verzeichnisse identifizieren

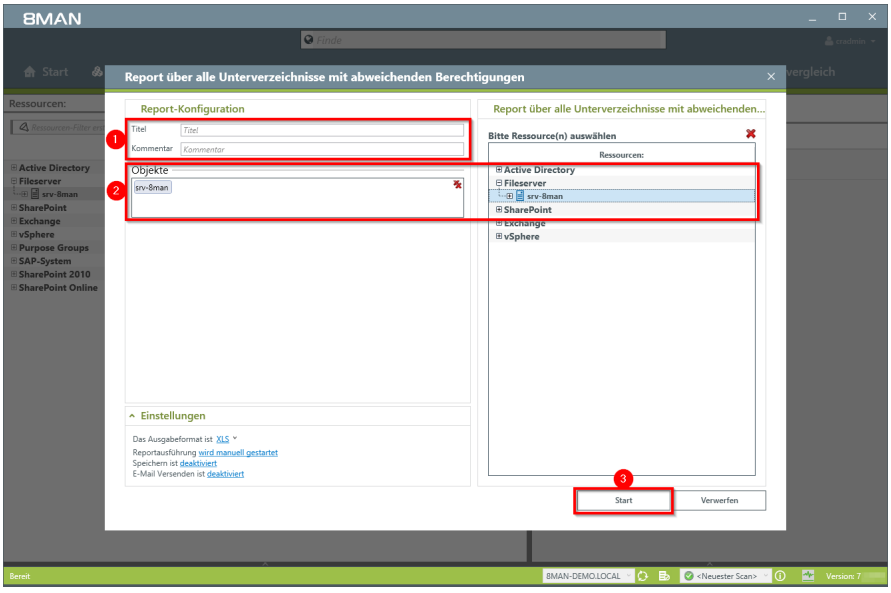
Hintergrund / Mehrwert

Die Rechtesituation auf dem Fileserver kann auf Unterverzeichnissen abweichen. 8MAN zeigt in einem Report die abweichenden Verzeichnisse. Unterbrochene Vererbungen sind häufig Ausdruck besonders geschützter Verzeichnisse.

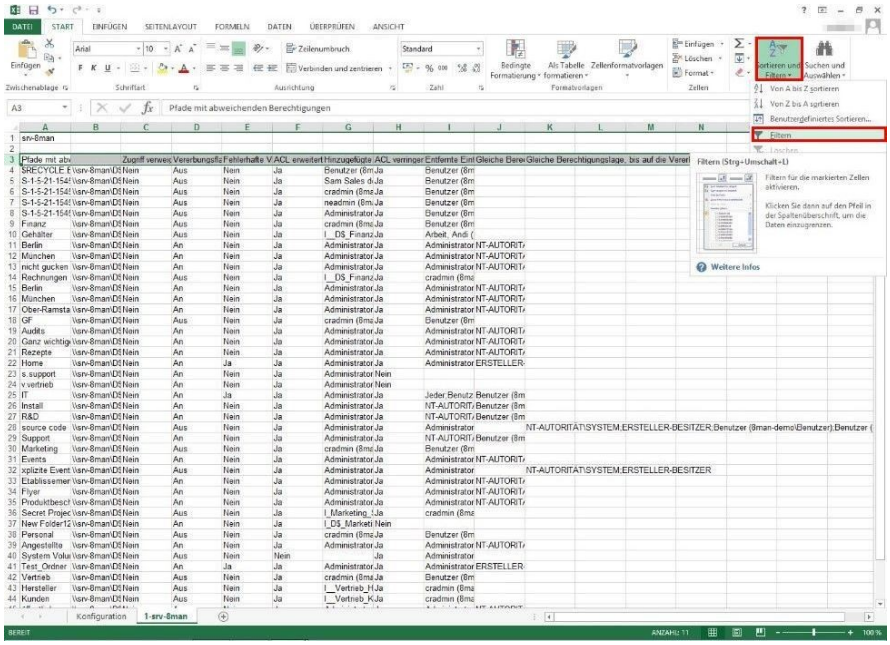
Der Prozess in einzelnen Schritten



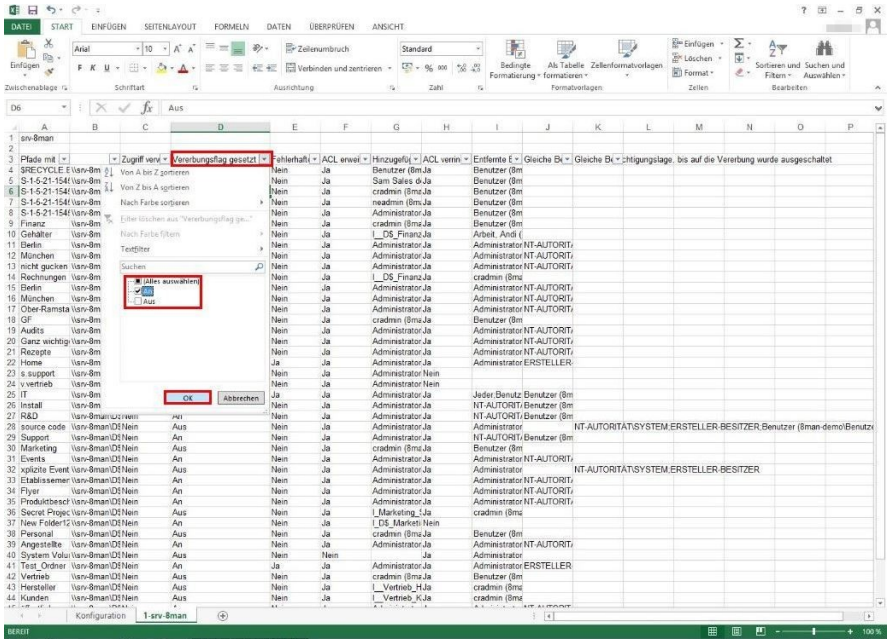
1. *Wählen Sie "Ressourcen".*
2. *Wählen Sie den gewünschten Fileserver.*
3. *Klicken Sie auf "Report".*
4. *Wählen Sie den "Report über alle Unterverzeichnisse mit abweichenden Berechtigungen".*



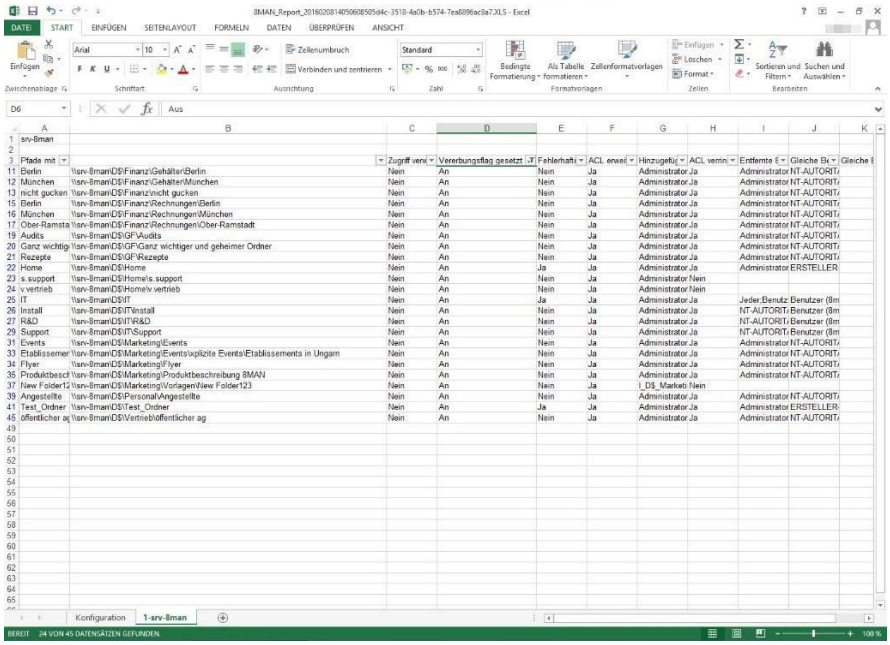
1. *Sie können dem Report einen Namen geben und einen Kommentar hinzufügen.*
2. *Ändern Sie ggf. den Umfang des Reports.*
3. *Starten Sie die Reporterstellung.*



Öffnen Sie die XLS-Datei mit Excel. Markieren Sie die oberste Zeile und fügen einen Filter ein.



Setzen Sie einen Filter in der Säule "Vererbungsflag gesetzt" auf "Aus".



Sie haben eine Liste aller Verzeichnisse, bei denen die Vererbung unterbrochen ist.

4.2.2.5 Berechtigungssituationen miteinander vergleichen (Scan Vergleich)

Hintergrund / Mehrwert

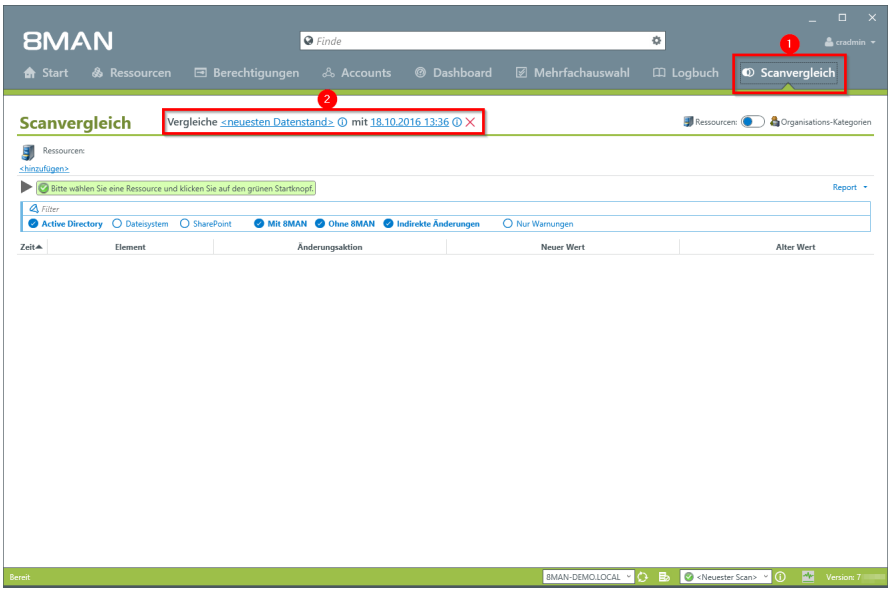
Der Scan-Vergleich zeigt die IST-Zustände von zwei Berechtigungssituationen auf dem Fileserver und vergleicht diese miteinander. Sie können somit feststellen, inwieweit sich Ihr Fileserver verändert hat.

Weiterführende Services:

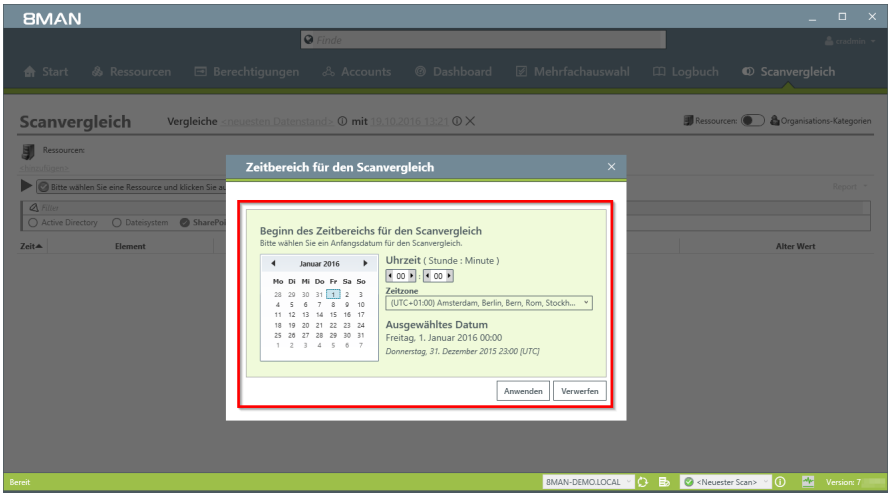
Der Vergleich bezieht nur zwei Messzeitpunkte in die Analyse ein. Um den gesamten IST-Prozess eines Zeitraumes zu identifizieren, benötigen Sie den im Security Monitoring aufgehängten FS Logga.

Nutzen Sie alternativ zum Scan-Vergleich den Berechtigungsdifferenzreport.

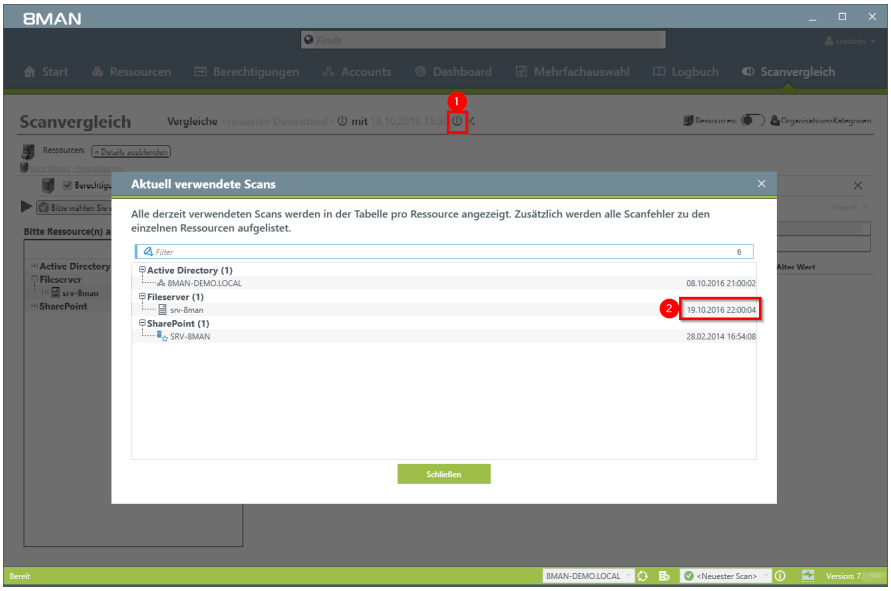
Der Prozess in einzelnen Schritten



1. *Klicken Sie auf den Menüpunkt "Scanvergleich".*
2. *Wählen Sie zwei Datenstände, die miteinander verglichen werden sollen.*



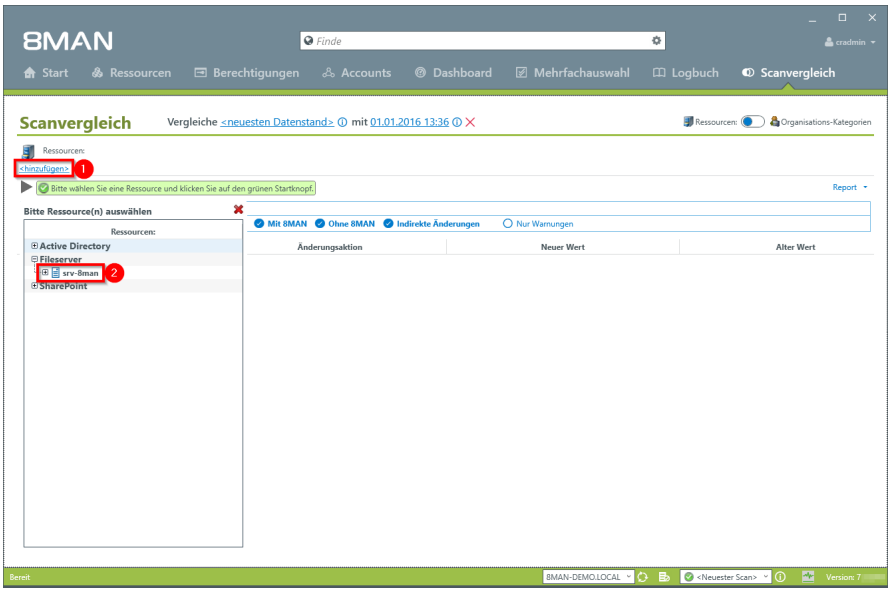
Wählen Sie Datum und Zeit für Anfang und Endpunkt.



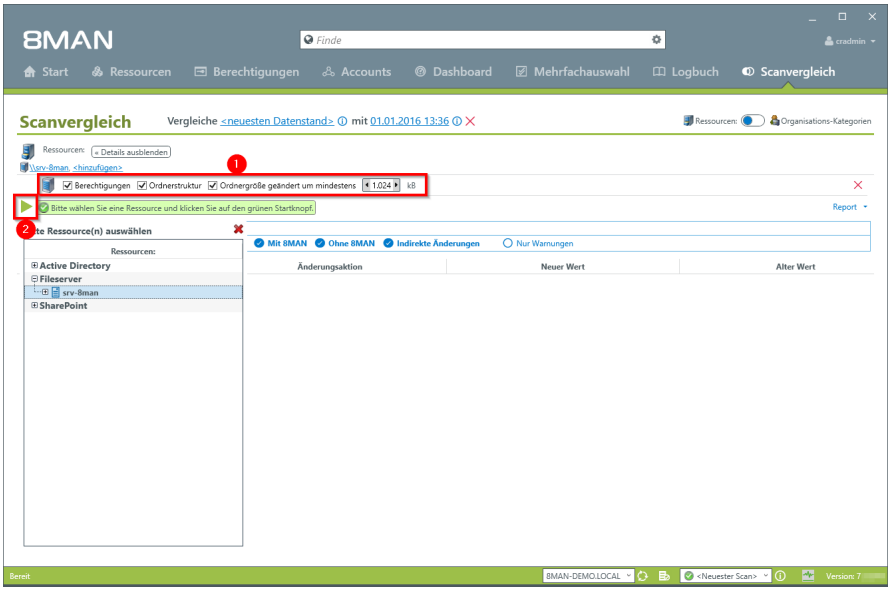
Der Vergleich bezieht sich immer auf vorhandene Scan-Datenstände.

1. *Klicken Sie auf das Informationssymbol.*
2. *8MAN zeigt Ihnen, welcher Scan-Datenstand für den Vergleich verwendet wird.*

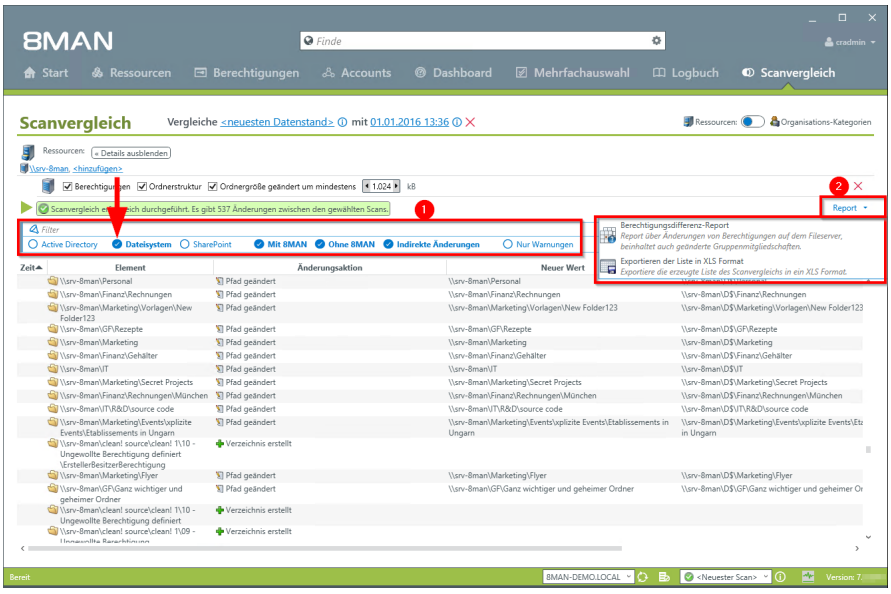
Führen Sie für ein möglichst aktuelles Ergebnis vorher einen neuen FS-Scan über die 8MAN Konfiguration aus.



1. *Klicken Sie auf Ressourcen hinzufügen.*
2. *Fügen Sie die gewählte Ressource mit Doppelklick hinzu.*



1. *Nachdem Sie alle zu prüfenden Ressourcen hinzugefügt haben, können Sie noch die zu erfassenden Parameter angeben.*
2. *Klicken Sie auf den Startknopf.*



Der Scanvergleich zeigt Ihnen die Ergebnisse.

1. *Sie können diese mit dem Filter eingrenzen.*
2. *Klicken Sie auf "Report". Sie können einen strukturierten Berechtigungsdifferenzreport generieren und / oder die vorliegenden Daten als .XLS Datei exportieren.*

4.2.2.6 Berechtigungssituationen aus der Vergangenheit analysieren

Hintergrund / Mehrwert

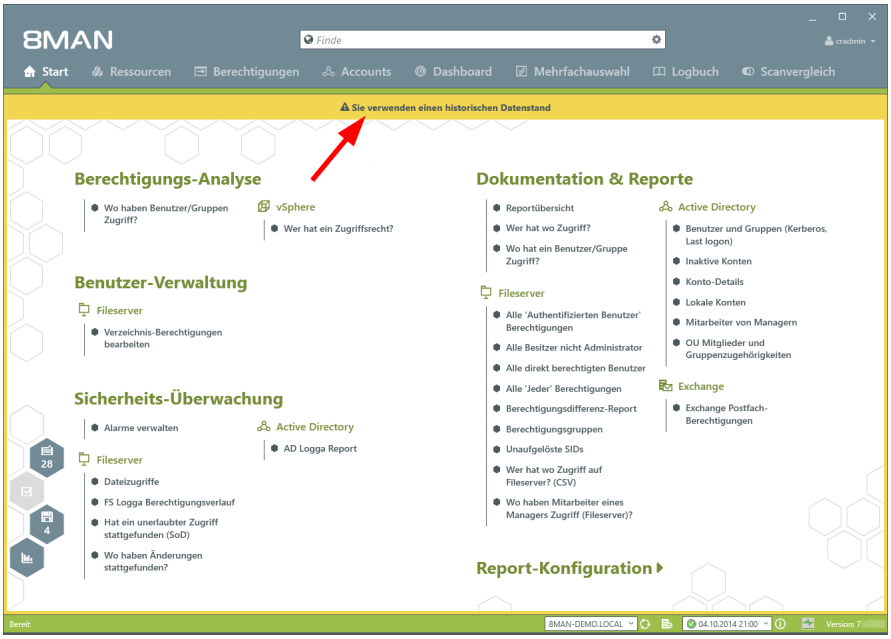
Nach Sicherheitsvorfällen empfielt sich ein Blick auf die Berechtigungssituation aus der Vergangenheit. Wer hatte Zugriff und wer ist aus systemischer Sicht entlastet?

Mit 8MAN können Sie alte Scans abrufen und im gewohnten "Look and Feel" die Situation zum Zeitpunkt der Erhebung auf dem Fileserver nachvollziehen.

Weiterführende Services

Alternativ können Sie auch zwei Scan Zeitpunkte miteinander vergleichen.

Der Prozess in einzelnen Schritten



Die Warnmeldung und der orange Rahmen signalisieren, dass Sie sich in der Vergangenheit bewegen.

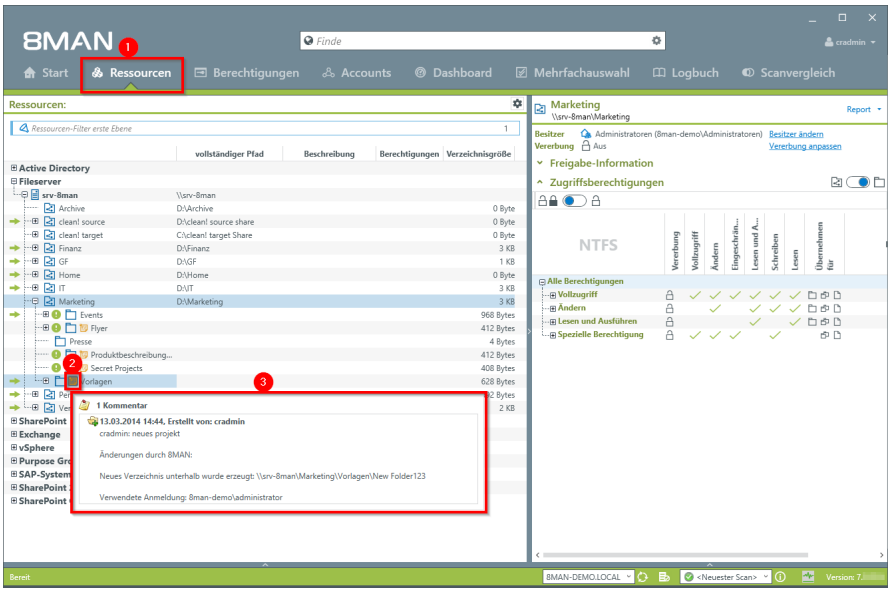
4.2.2.7 Die letzten Aktionen an einem Verzeichnis identifizieren

Hintergrund / Mehrwert

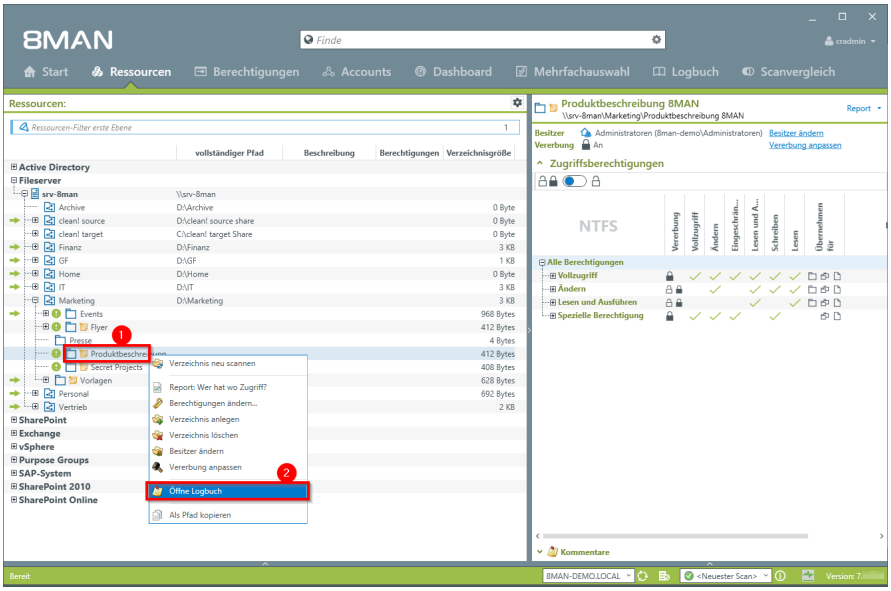
Fileserver-Verzeichnisse haben eine eigene Historie. Deshalb macht es Sinn vor der weiteren Bearbeitung zu prüfen, was vorher durchgeführte Aktivitäten waren.

8MAN zeigt in einer Schnellansicht die letzten Aktivitäten oder Sie gelangen direkt in das Logbuch, um eine vollständige Auflistung zu erhalten.

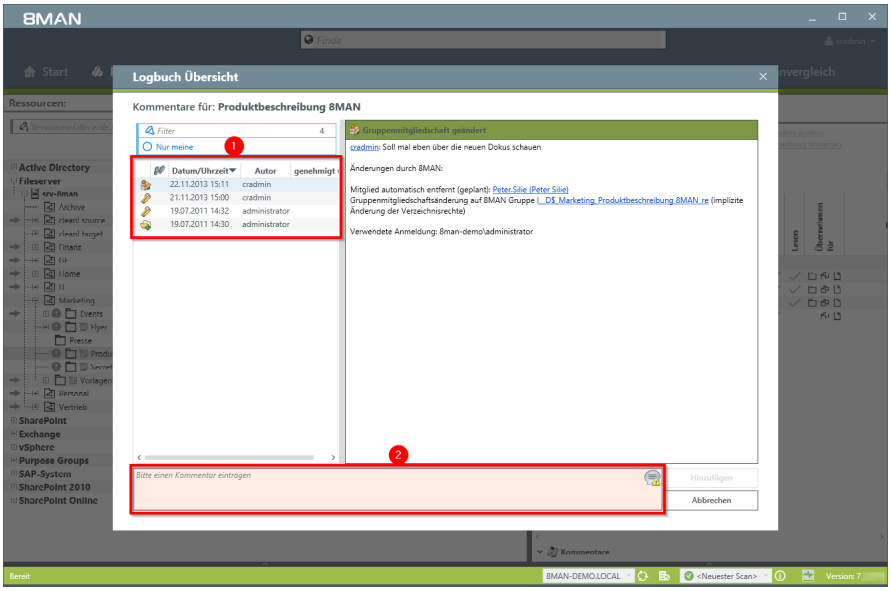
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Das Notizzettelsymbol zeigt Ihnen, dass in 8MAN Kommentare hinterlegt sind. Fahren Sie mit der Maus über ein Symbol.*
3. *8MAN zeigt eine Schnellansicht der letzten Aktionen.*



1. *Wählen Sie ein Verzeichnis mit Rechtsklick.*
2. *Klicken Sie auf "Öffne Logbuch".*



1. *Prüfen Sie die am Objekt bereits durchgeführten Aktivitäten.*
2. *Sie können einen Kommentar in das Logbuch schreiben.*

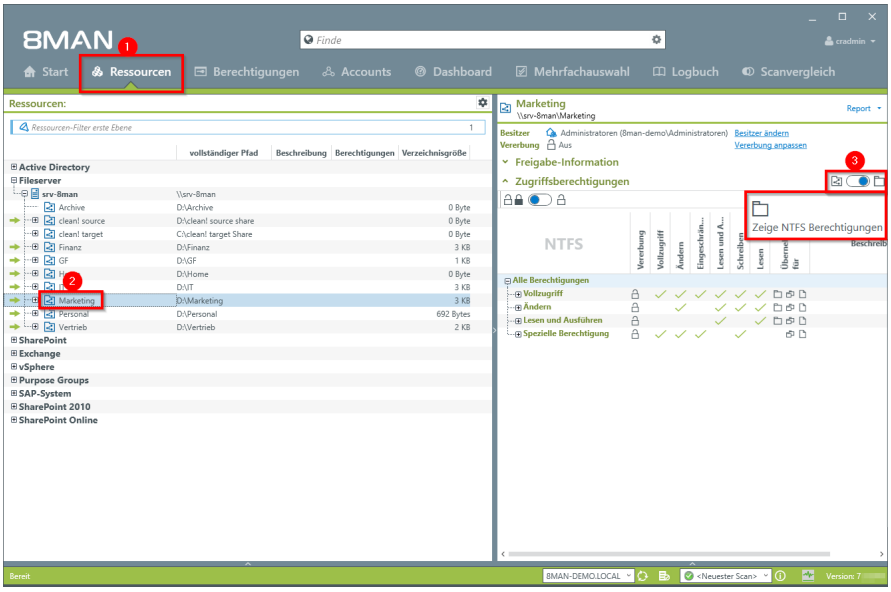
4.2.2.8 Share Berechtigungen identifizieren

Hintergrund / Mehrwert

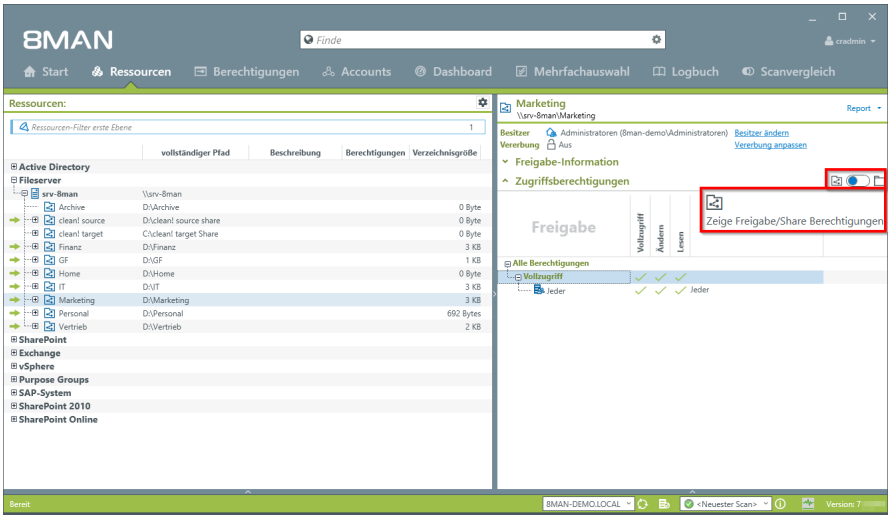
8MAN zeigt für Freigabe-Verzeichnisse sowohl die Freigabe- Berechtigungen als auch die NTFS-Berechtigungen. Im Standard werden die NTFS-Berechtigungen angezeigt.

Im Verhältnis zwischen Freigabe-Berechtigungen und NTFS-Berechtigungen sind immer die geringeren Rechte für den Nutzer ausschlaggebend. Deshalb empfehlen wir bei Freigabe-Berechtigungen immer Vollzugriff einzustellen und dann über die NTFS-Berechtigungen feingranularer Rechte zu vergeben.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Wählen Sie ein Freigabe-Verzeichnis.*
3. *8MAN zeigt standardmäßig die NTFS-Berechtigungen.*



Klicken Sie auf den Schiebeschalter, um zwischen der Anzeige der Share- und der NTFS-Berechtigungen hin- und herzuschalten.

4.3 +8MATE for Exchange

Mit dem 8MATE for Exchange erweitern Sie ihren 8MAN für Exchange-Ressourcen. Damit erfolgt die Analyse und Administration von Berechtigungen zentral und im Einklang mit dem Access Management für andere Anwendungen. In der gewohnten 8MAN Übersicht sehen Sie auf einen Blick, wer auf Postfächer, Verteilergruppen, öffentliche Ordner, Kontakte, Postfachordner und z. B. Kalender zugreifen kann.

Die Administration von Exchange ist eng an den Onboarding-Prozess angelegt: Die Anlage von Postfächern, Verteilergruppen, Kontakten und die Vergabe von Zugriffsrechten erfolgt direkt im 8MAN. Änderungen werden revisionssicher im 8MAN dokumentiert.

Neben der Analyse und Administration von Berechtigungen im Exchange verfügt der 8MATE über weitere Features:

- Abwesenheitsnotizen ändern
- Eigenschaften von Postfächern identifizieren
- Postfachgrößen administrieren
- Verteilergruppen verwalten, einschließlich Berechtigungen, Mitglieder, Manager und Moderatoren
- Kontakten verwalten
- Verwaltung von Postfächern
- E-Mail-Adressen bearbeiten

An den Postfächern, Verteilergruppen, Kontakten und E-Mail-aktivierten öffentlichen Ordnern werden folgende Berechtigungen gelesen:

- Senden als
- Empfangen als (nicht bei Exchange Online)
- Senden im Auftrag von
- Moderation
- Manager (nur bei Verteilergruppen)
- ms-exch-epi-may-impersonate (nicht bei Exchange Online)

Folgende zusätzlichen Informationen werden zu jedem Postfach abgerufen:

- Postfachweiterleitungen
- aktivierte Abwesenheitsnotizen ohne Nachrichtentext
- Stellvertretungen
- Vollzugriffsberechtigungen

Der Ordnertyp von benutzerdefinierten Postfachordnern kann in der PowerShell nicht festgestellt werden. Ordnertypen für benutzerdefinierte Postfachordner stehen deshalb nicht zur Verfügung.

4.3.1 Help Desk

4.3.1.1 Die Zugriffsrechte auf Postfächer zeigen

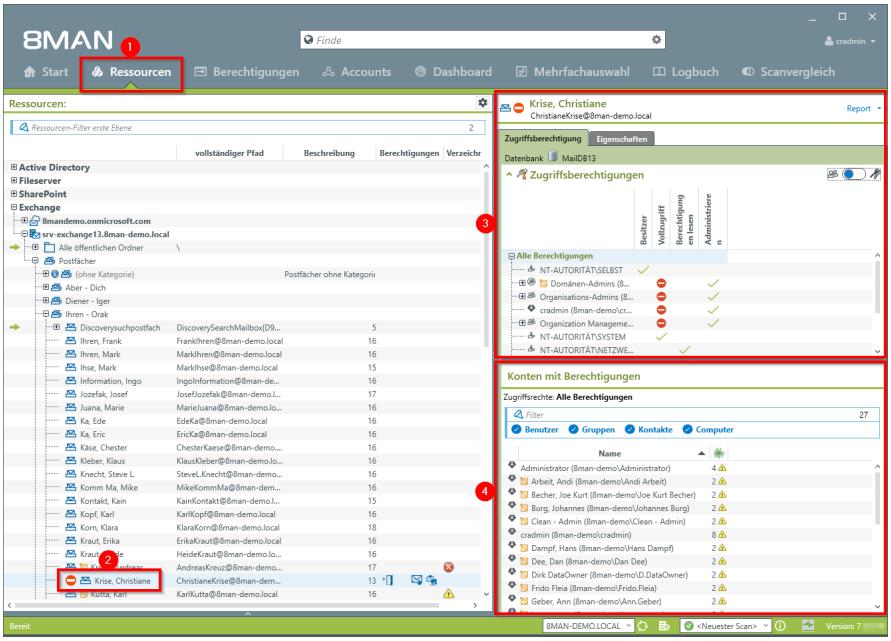
Hintergrund / Mehrwert

Wer kann auf welche Postfächer zugreifen? Der 8MATE Exchange zeigt die Zugriffsrechte in der Ressource-Ansicht. Unterschieden wird zwischen "Besitzer", "Vollzugriff" , "Berechtigungen lesen", "Administrieren", "Senden als", "Senden im Auftrag von" und "Empfangen als".

Weiterführende Services

Alternativ können Sie den Report "Wer hat wo Zugriff" die Zugriffsrechte auf Postfächer erfassen. Differenzierter ist der Report "Postfachberechtigungen identifizieren"

Der Prozess in einzelnen Schritten



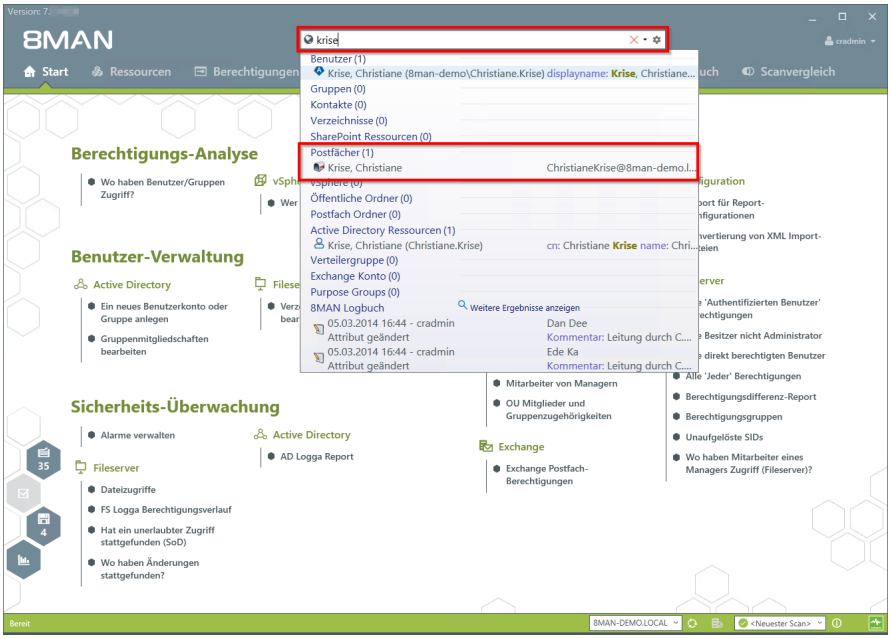
1. *Wählen Sie "Ressourcen".*
2. *Navigieren Sie zum gewünschten Postfach.*
3. *8MAN zeigt Ihnen, welche Benutzer/Gruppen welche Rechte haben.*
4. *8MAN zeigt berechtigte Konten in einer flachen Liste.*

4.3.1.2 Eigenschaften von Postfächern identifizieren

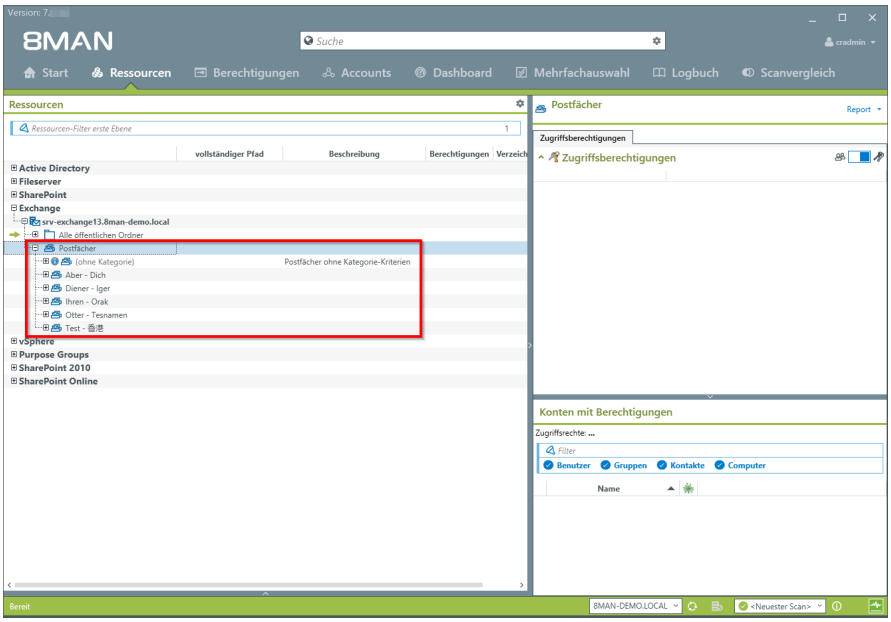
Hintergrund / Mehrwert

8MAN identifiziert Eigenschaften von Postfächern und stellt diese übersichtlich dar. Insbesondere auch sicherheitskritische Eigenschaften wie "Senden als", bei denen der Verfasser nicht mehr als anderer Autor erkennbar ist. Prüfen Sie deshalb genau wer in Namen von wem Nachrichten verschicken darf.

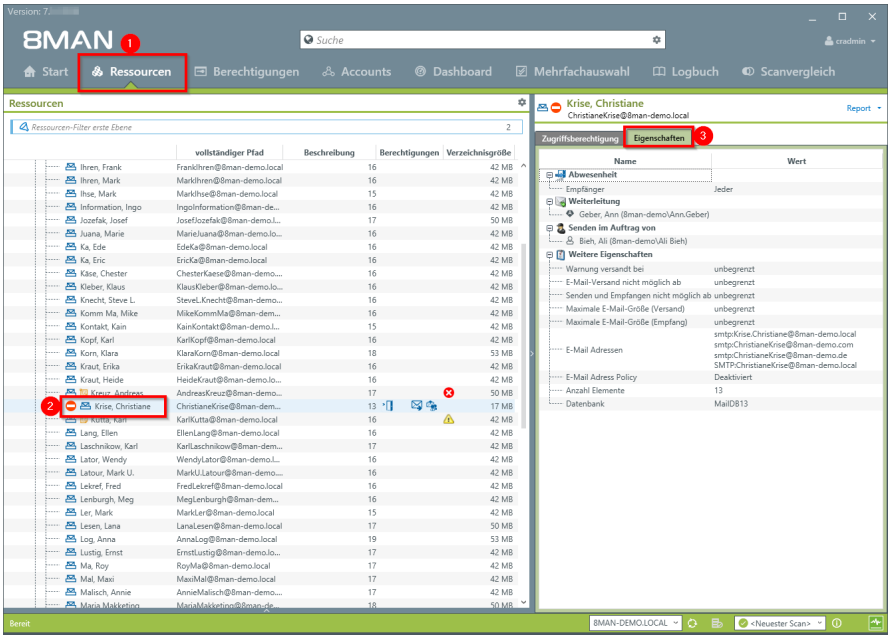
Der Prozess in einzelnen Schritten



Nutzen Sie die Suche, um das gewünschte Postfach zu finden.



Ab einer Anzahl von 200 Postfächern gruppiert 8MAN die Postfächer. Dadurch wird die Übersicht in der Anzeige gewährleistet. Die Aufteilung geschieht auf Basis des Nachnamens. Die Gruppierungseinstellungen können angepasst werden, siehe Kapitel "erweiterte Exchange Scaneinstellungen in den Konfigurationsdateien".



1. *8MAN wechselt automatisch in die Ressourcen-Ansicht.*
2. *Sie haben das gewünschte Postfach im Fokus.*
3. *Klicken Sie auf den Reiter Eigenschaften.*

4.3.1.3 Die Zugriffsrechte auf öffentliche Ordner identifizieren

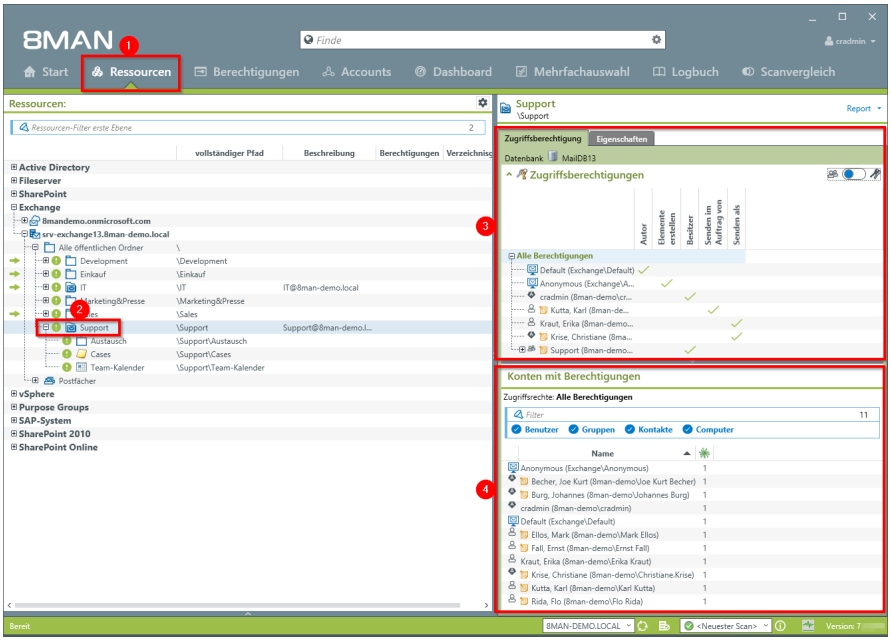
Hintergrund / Mehrwert

Die Berechtigungen auf öffentliche Ordner im Blick zu behalten ist mit Bordmitteln komplex. Mit 8MAN sehen Sie in der Ressourcen-Ansicht die Rechtesituation auf öffentliche Ordner.

Weiterführende Services

Report: Wer hat wo Zugriff?
Report: Postfach Berechtigungen identifizieren
Ein Postfach anlegen
Berechtigungen auf Postfächer ändern
Abwesenheitsnotizen ändern
Postfachgrößen ändern

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Navigieren Sie zum gewünschten öffentlichen Ordner.*
3. *8MAN zeigt Ihnen, welche Benutzer/Gruppen welche Rechte haben.*
4. *8MAN zeigt berechtigte Accounts in einer flachen Liste.*

4.3.1.4 Berechtigungen auf Verteilergruppen anzeigen

Hintergrund / Mehrwert

Mit 8MAN können Sie schnell prüfen, wer über welchen Verteiler E-Mails verschicken kann.

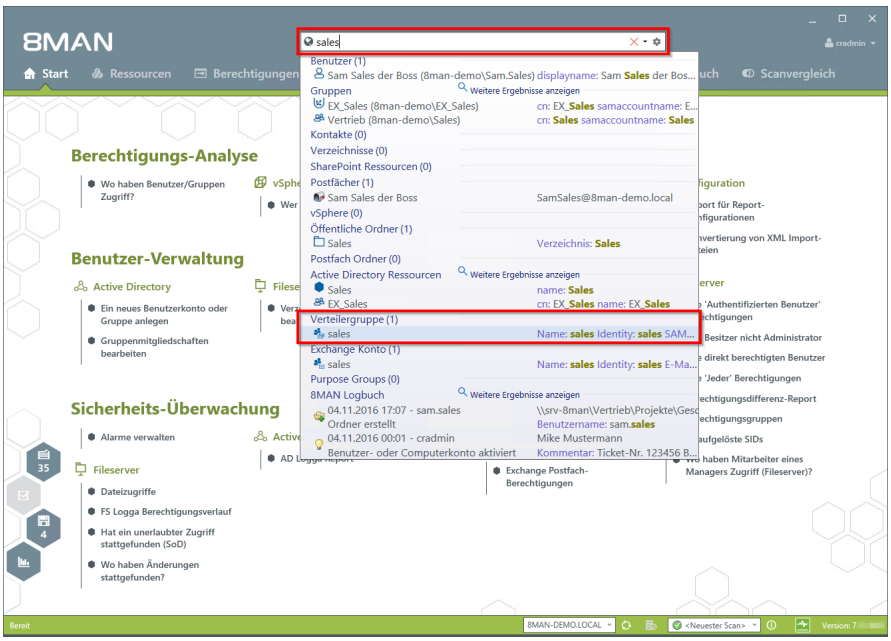
Relevant sind die beiden Fälle „Senden als“ und „Senden im Auftrag von“:

Der Erstgenannte ist besonders brisant, weil nicht ersichtlich ist, wer tatsächlich die E-Mail verschickt hat.

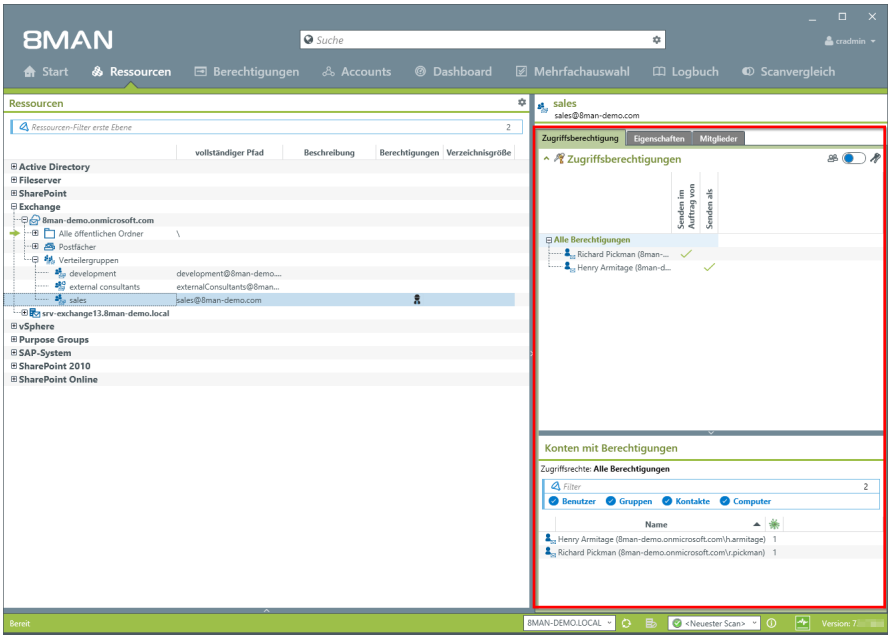
Bei „Senden im Auftrag von“ ist z. B. der Sekretär / die Sekretärin, die im Auftrag versendet, für den Empfänger erkennbar.

Die Anzeige funktioniert auch bei dynamischen Exchange-Gruppen.

Der Prozess in einzelnen Schritten



Nutzen Sie die Suche, um die gewünschte Verteilergruppe zu finden.



8MAN zeigt die Zugriffsberechtigungen.

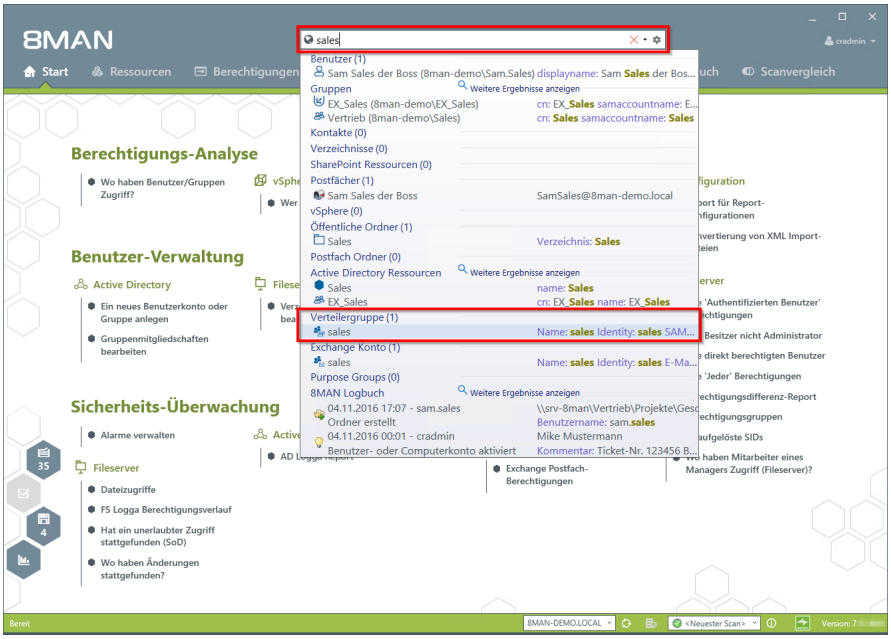
4.3.1.5 Mitglieder von Verteilergruppen anzeigen

Hintergrund / Mehrwert

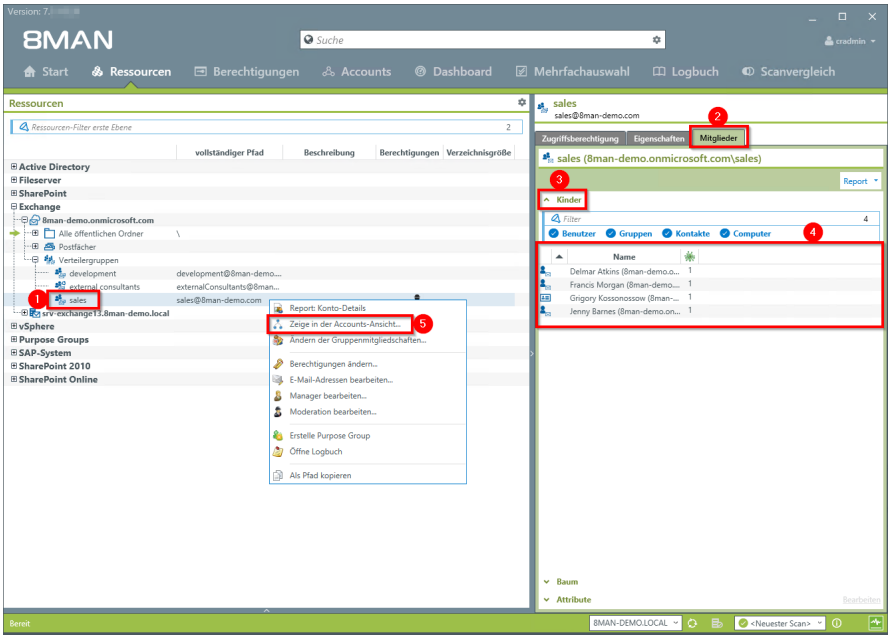
Mit 8MAN können Sie die Empfänger bzw. Mitglieder von Verteilern anzeigen. Dabei werden 8MAN-typisch auch Gruppenverschachtelungen berücksichtigt angezeigt.

Die Anzeige funktioniert auch bei dynamischen Exchange-Gruppen.

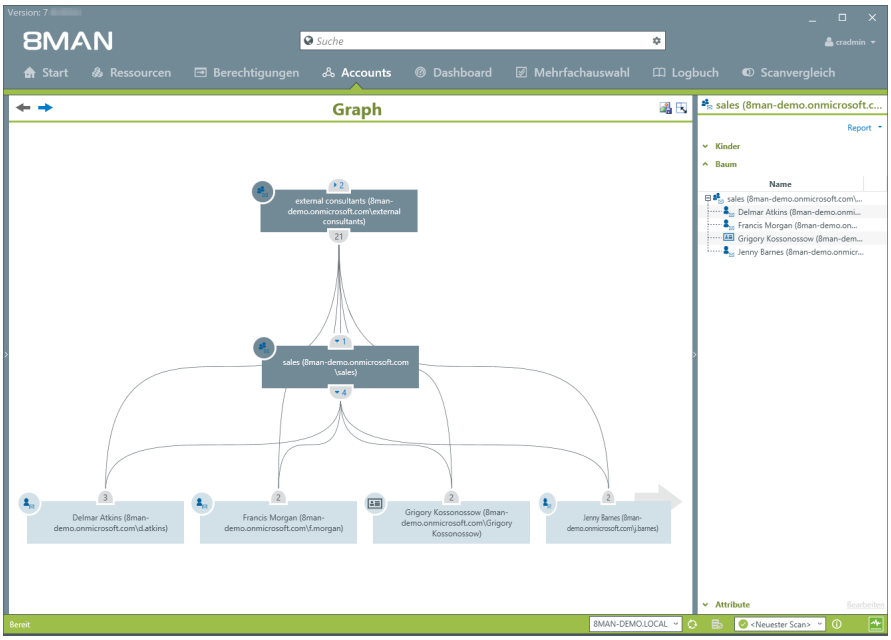
Der Prozess in einzelnen Schritten



Nutzen Sie die Suche, um die gewünschte Verteilergruppe zu finden.



1. *Nehmen Sie die Verteilergruppe in den Fokus.*
2. *Wählen Sie den Reiter "Mitglieder".*
3. *Klappen Sie den Bereich "Kinder" auf.*
4. *Sie sehen alle Mitglieder der Verteilergruppe in einer flachen Liste.*
5. *Alternativ können Sie die Gruppe auch in der Accounts-Ansicht analysieren. Rechtsklicken Sie auf die Verteilergruppe und wählen "Zeige in der Accounts-Ansicht..." im Kontextmenü.*



Nutzen Sie die Account-Ansicht, um Verschachtelungen und Mitgliedschaften zu analysieren.

4.4 +8MATE for SharePoint

Der 8MATE for SharePoint integriert sämtliche SharePoint-Ressourcen in Ihren 8MAN. Damit erfolgt die Analyse und Administration von Berechtigungen zentral und im Einklang mit dem Access Management für andere Anwendungen. Sie profitieren von der Analyse- und Darstellungskompetenz des 8MAN und können Zugangsrechte schnell verändern.

8MAN zeigt die Berechtigungen in einer Baumstruktur an. Damit sehen Sie schnell, wer auf welche SharePoint Ressource zugreifen kann. Über den Scanvergleich-Report erfahren Sie, wer welche Änderungen an Berechtigungen durchgeführt hat und erhalten ein revisionssicheres Protokoll vorgenommener Aktivitäten.

Mit dem 8MATE for SharePoint können Sie in der 8MAN Oberfläche alle Berechtigungen vergeben. Mit dem Group Wizard und der Vergabe von Namenskonventionen standardisieren Sie Ihren Berechtigungsvergabeprozess.

4.4.1 Services für Administratoren und Data Owners

4.4.1.1 Zugriffsrechte auf SharePoint Ressourcen identifizieren

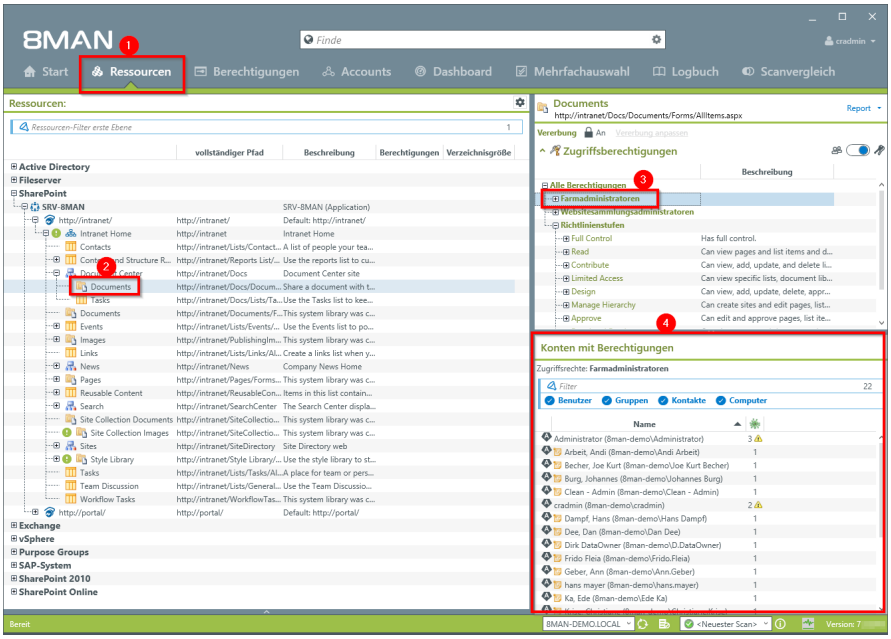
Hintergrund / Mehrwert

Der 8MATE for SharePoint identifiziert sämtliche Zugriffsrechte auf Sharepoint Ressourcen im gewohnten Look & Feel der Ressourcenansicht.
Damit erfolgt die Analyse zentral und im Einklang mit dem Access Rights Management für andere Anwendungen.

Weiterführende Services

Report: Wer hat wo Zugriff?
Report: Wo haben Benutzer/Gruppen Zugriff?
Berechtigungen auf SharePoint Ressourcen ändern
Namenskonventionen bei der Berechtigungsvergabe über AD Gruppen festlegen

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Navigieren Sie zur gewünschten SharePoint Ressource.*
3. *Wählen Sie eine Zugriffsberechtigung.*
4. *8MAN zeigt die berechtigten Accounts in einer flachen Liste.*

4.4.2 Services für Administratoren

4.4.2.1 Abweichende Berechtigungen in der Baumstruktur identifizieren

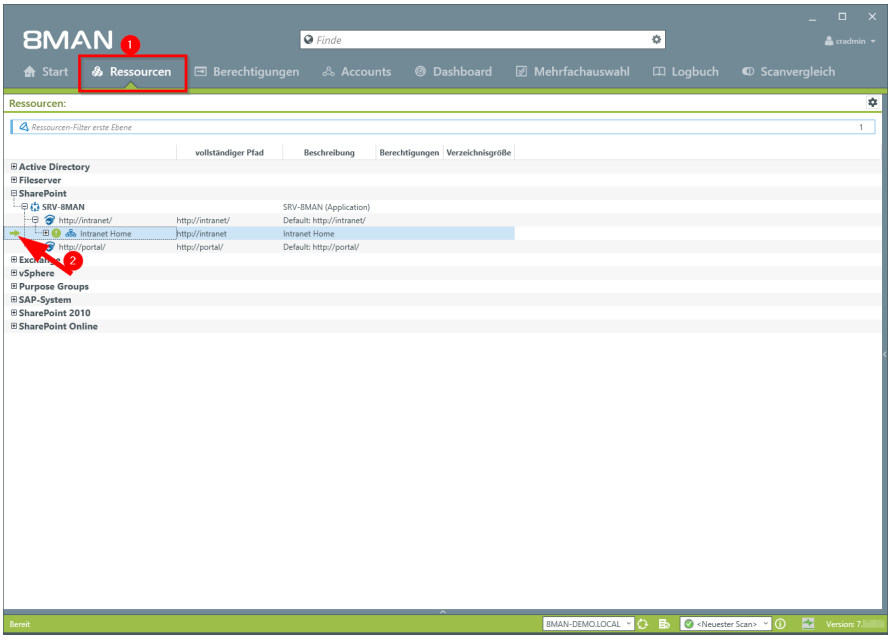
Hintergrund / Mehrwert

Wie bei Fileservern werden Zugriffsrechte auch bei SharePoint vererbt. 8MAN zeigt abweichende Berechtigungen an - sowohl entfernte als auch hinzugefügte. Ist die Vererbung unterbrochen und die Rechtesituation dadurch abweichend, zeigt 8MAN dies in der SharePoint Baumstruktur an. Sie können die abweichenden Rechte angleichen, oder sofern die Ressource besonders geschützt sein soll, bestehen lassen.

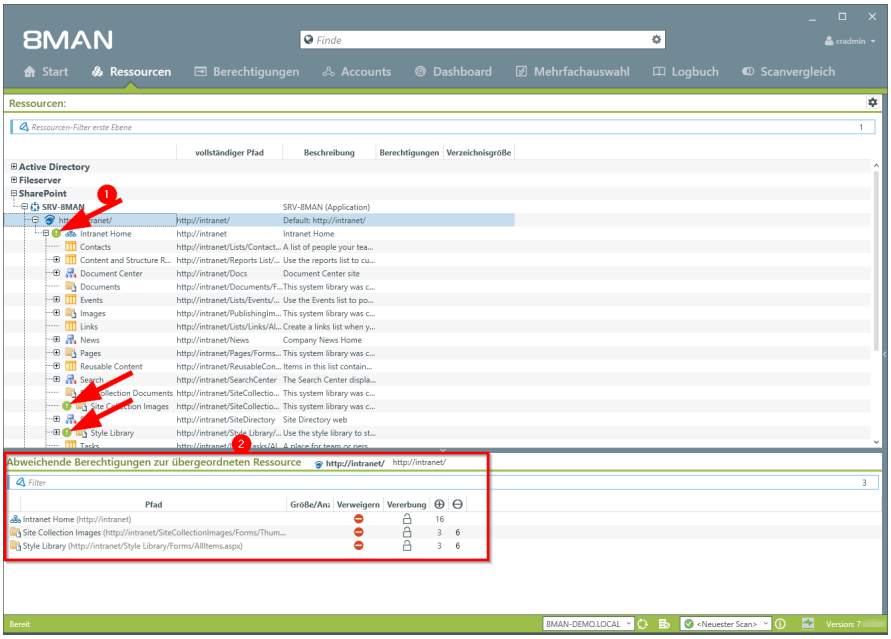
Weiterführende Services

Report: Wer hat wo Zugriff?
Report: Wo haben Benutzer/Gruppen Zugriff?
Berechtigungen auf SharePoint Ressourcen ändern
Namenskonventionen bei der Berechtigungsvergabe über AD Gruppen festlegen

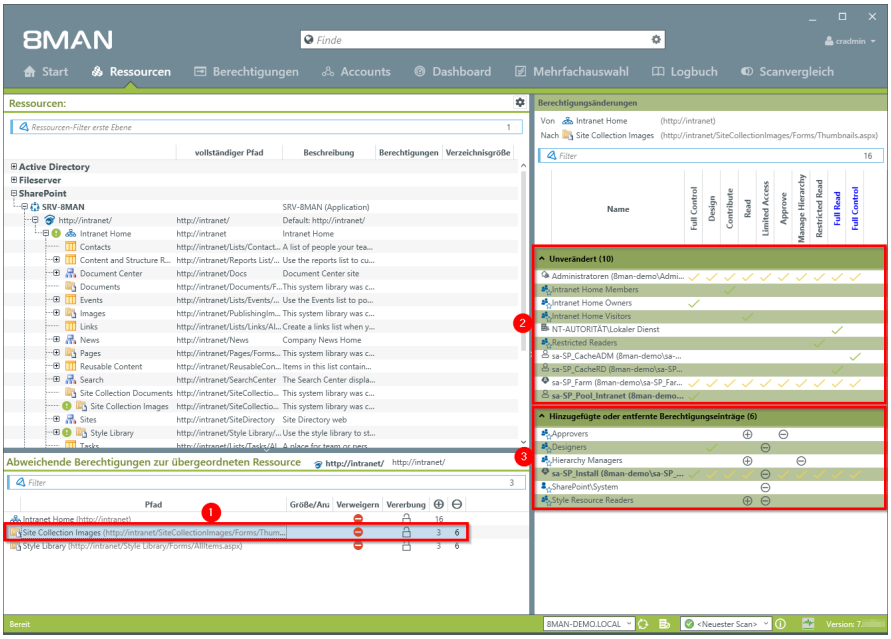
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Der grüne Pfeil zeigt an, dass Unterverzeichnisse mit abweichenden Berechtigungen vorhanden sind.*



1. *Der grüne Kreis mit dem Ausrufezeichen zeigt an, dass bei diesem Verzeichnis die Berechtigung vom übergeordneten abweicht.*
2. *Die Verzeichnisse mit abweichenden Berechtigungen werden im unteren aufklappbaren Fenster aufgelistet.*



1. *Selektieren Sie ein Unterverzeichnis.*
2. *8MAN zeigt alle Berechtigungen, die mit denen des übergeordneten Verzeichnisses übereinstimmen.*
3. *8MAN zeigt alle abweichenden Berechtigungen. Ein "Plus" steht für hinzugefügte, ein "Minus" für entfernte Berechtigungen.*

4.5 +8MATE for Dynamics NAV

4.5.1 Dynamics NAV Berechtigungen analysieren

Microsoft Dynamics NAV beinhaltet unternehmerische Informationen, die nicht jeder sehen sollte. Je nach Ausbaustufe der ERP-Lösung sind dort Projektbudgets, EK-Preislisten, Jahresbilanzen oder personenbezogene Daten von Mitarbeitern, Lieferanten oder Kunden hinterlegt.

Ein effizientes Berechtigungsmanagement ist mit Bordmitteln schwierig. Nutzer sind Mitglied in verschiedenen Berechtigungsgruppen, die wiederum Mitglied in weiteren Berechtigungsgruppen sein können. Darüber hinaus nutzt die ERP-Lösung unternehmensspezifische Berechtigungssätze, über die ebenfalls Zugriffsrechte vergeben werden. Möchte man wissen, welche Nutzer welche Zugriffsrechte haben, müssen entsprechend viele Quellen konsolidiert werden. Die Antwort auf die eigentlich sehr einfache Frage: „Wer hat wo Zugriff?“, wird zu einem kostspieligen und zeitintensiven Suchprojekt.

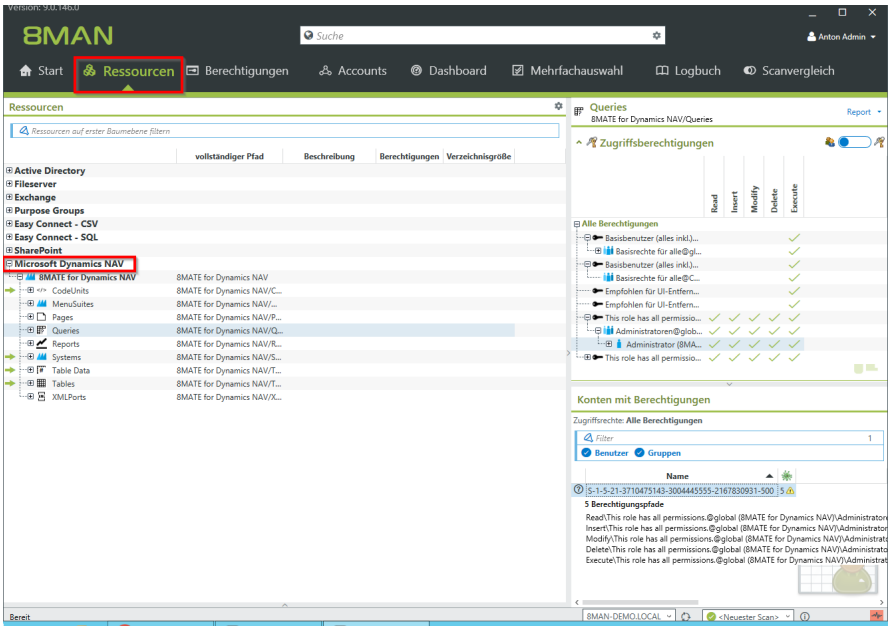
Das 8Mate Dynamics NAV integriert die Berechtigungsanalyse des ERP-Systems in 8MAN. In gewohnter Weise sehen Sie alle Zugriffsrechte in einer flachen Liste. Im ersten Schritt bietet das Modul Services im Bereich Permission Analysis und Documentation & Reporting:

Permission Analysis

- Zugriffsrechte auf NAV Ressourcen identifizieren
- Mehrfachberechtigungen identifizieren
- Die Berechtigungssituation aus der Vergangenheit analysieren

Documentation & Reporting

- Report: Wer hat wo Zugriff?
- Report: Wo haben Benutzer/Gruppen Zugriff?



Navigieren Sie in "Ressourcen" zu "Microsoft Dynamics NAV". Alle Berechtigungen werden 8MAN-typisch angezeigt.

5. Documentation & Reporting

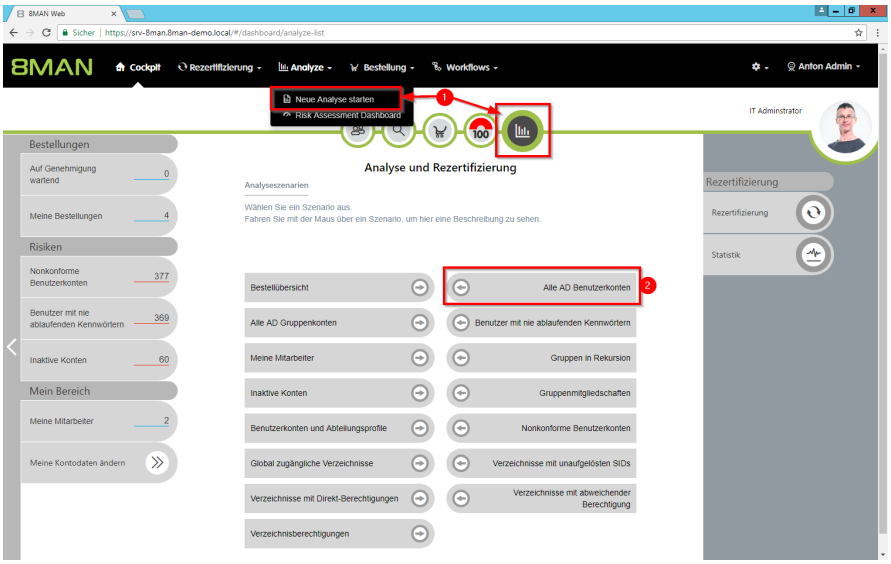
5.1 Alle Technologien

5.1.1 Flexible Reporte (Webclient)

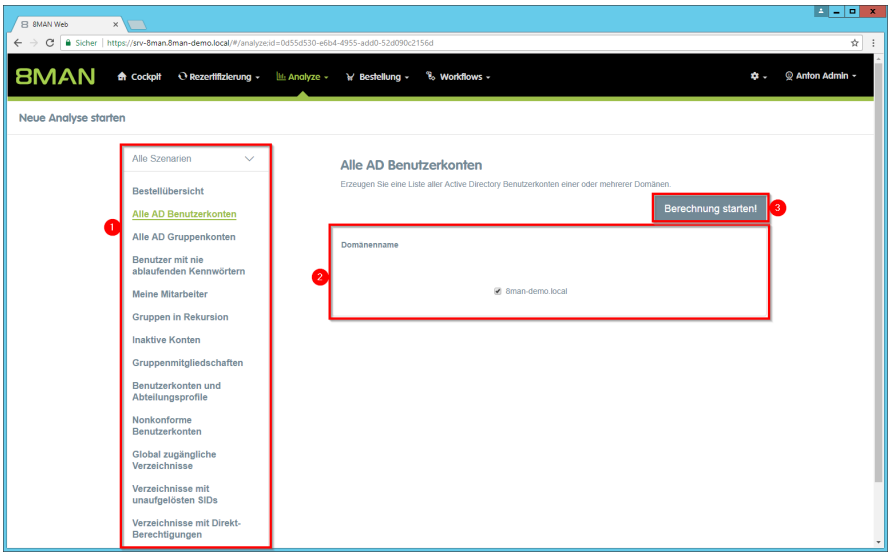
Hintergrund / Mehrwert

Mit Analyze & Act erstellen Sie über den Webclient flexible Reporte. Designen Sie den Report mit Gruppierungen, Filtern, Sortierungen und der Auswahl der gewünschten Spalten genau so, wie Sie ihn brauchen. Den fertig gestalteten Report exportieren Sie dann z. B. direkt ins Excel-Format.

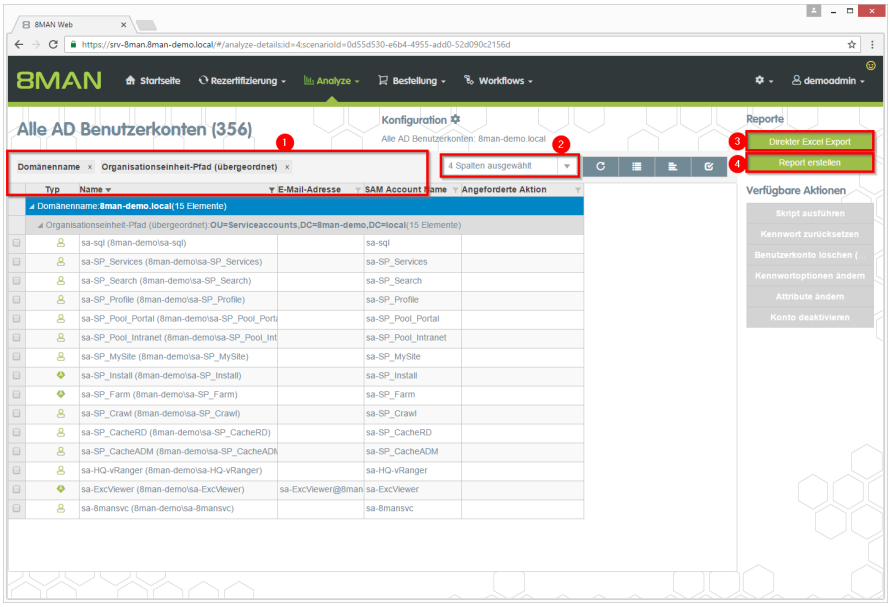
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Alle AD Benutzerkonten".*



1. *Optional: Wechseln Sie das Szenario.*
2. *Legen Sie Optionen für das Szenario fest.*
3. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie Gruppierungen, Sortierungen und Filter um den Reportinhalt festzulegen.*
2. *Wählen Sie die Spalten für den Report aus.*
3. *Exportieren Sie den Report direkt ins Excel-Format.*
4. *Erstellen Sie einen Report im PDF oder CSV-Format, den Sie auf dem Dateisystem speichern oder per E-Mail versenden.*

5.1.2 8MAN Access Rights Management Aktivitäten berichten (Logbuch Report)

Hintergrund / Mehrwert

Alle Änderungen, die Sie mit 8MAN Enterprise vornehmen, werden im Logbuch automatisch erfasst. Damit erfüllt 8MAN die Kriterien der Revisionssicherheit und entlastet Sie von händischer Dokumentation.

Der Logbuch-Report ermöglicht es, die Events nach Personen oder Eventart in einem beliebigen Zeitraum zu erfassen. Dadurch erhalten Sie vollständige Prozesstransparenz.

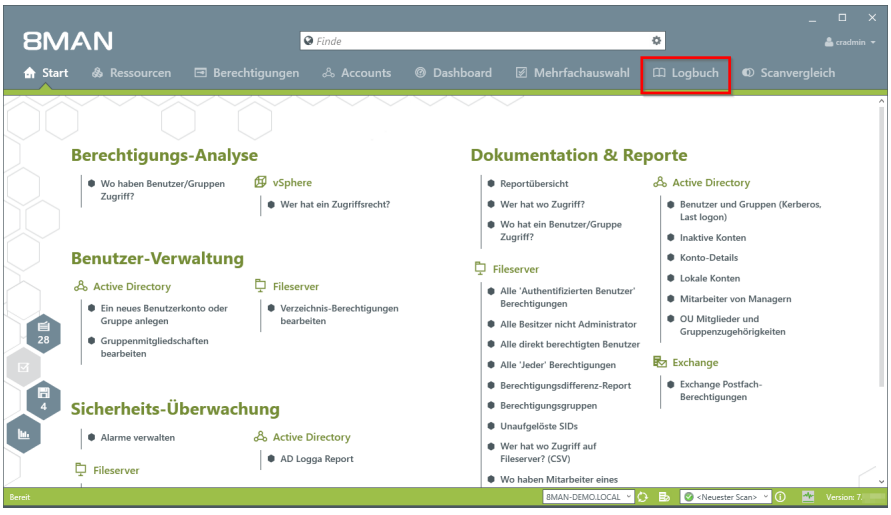
Sofern Sie über eine Visor Lizenz in Verbindung mit dem 8MATE AD Logga verfügen, wird das Logbuch mit AD Events gefüllt.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen sowie M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen.

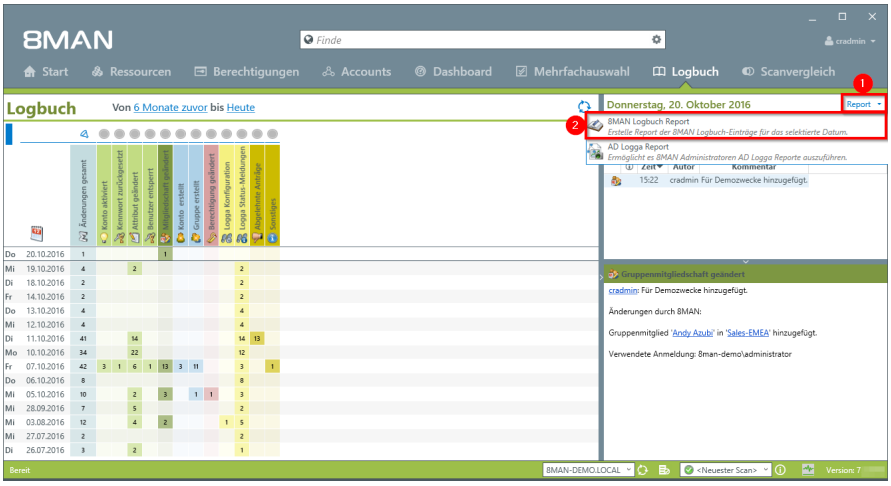
Ähnliche Services

Mit dem Security Monitoring erweitert 8MAN die Protokollierung: Auch Aktivitäten die außerhalb von 8MAN angestoßen wurden, sind darin enthalten.

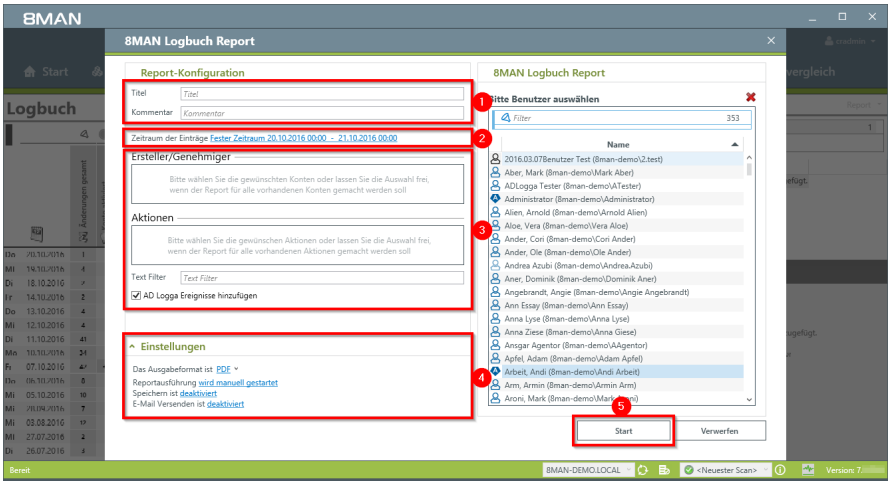
Der Prozess in einzelnen Schritten



Wählen Sie "Logbuch".



1. *Klicken Sie auf Report.*
2. *Wählen Sie "8MAN Logbuch Report".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Legen Sie den Zeitraum fest, über den berichtet werden soll.*
3. *Definieren Sie den Umfang des Reports.*
4. *Legen Sie verschiedene Ausgabeoptionen fest.*
5. *Starten Sie die Erstellung des Reports.*

5.2 Active Directory

5.2.1 Reporte für Führungskräfte

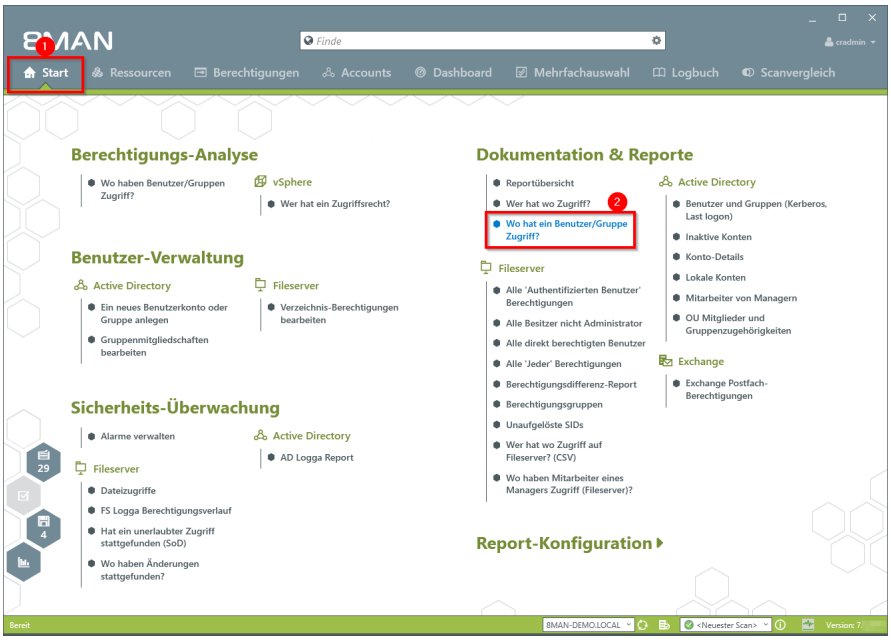
5.2.1.1 Wo haben Benutzer/Gruppen Zugriff?

Hintergrund / Mehrwert

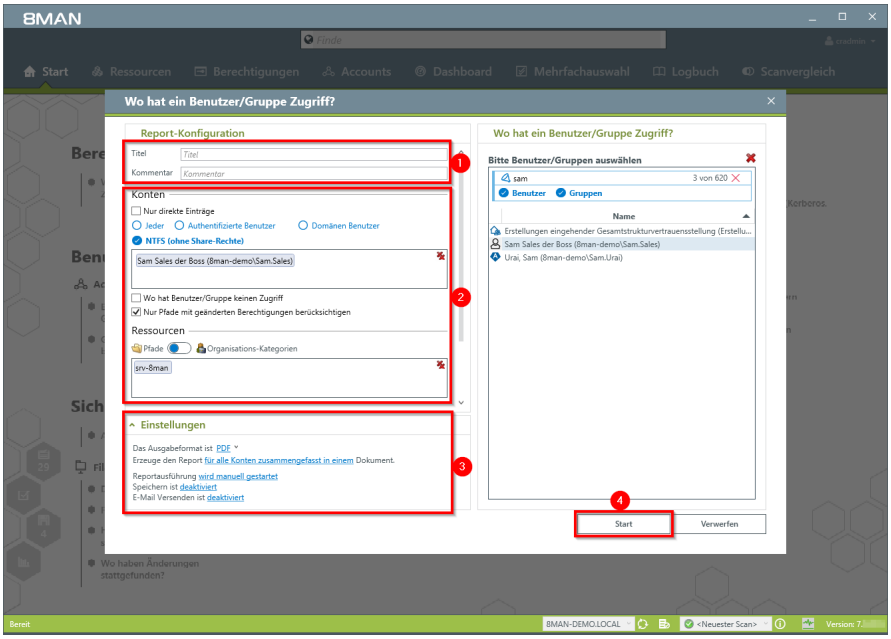
Der Report "Wo hat ein Benutzer/Gruppe Zugriff?" listet die Zugriffsrechte von Nutzerkonten und Gruppen auf ausgewählten Fileserver-Verzeichnissen in einem Dokument auf.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle, M 2.8 Vergabe von Zugriffsrechten sowie M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start"*
2. *Klicken Sie auf "Wo hat eine Benutzer/Gruppe" Zugriff?*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.2.1.2 Mitarbeiter von Managern

Hintergrund / Mehrwert

Data Owner, die über Active Directory Kenntnisse verfügen, können sich die Attribute und Gruppenzugehörigkeiten Ihrer Mitarbeiter anzeigen lassen.

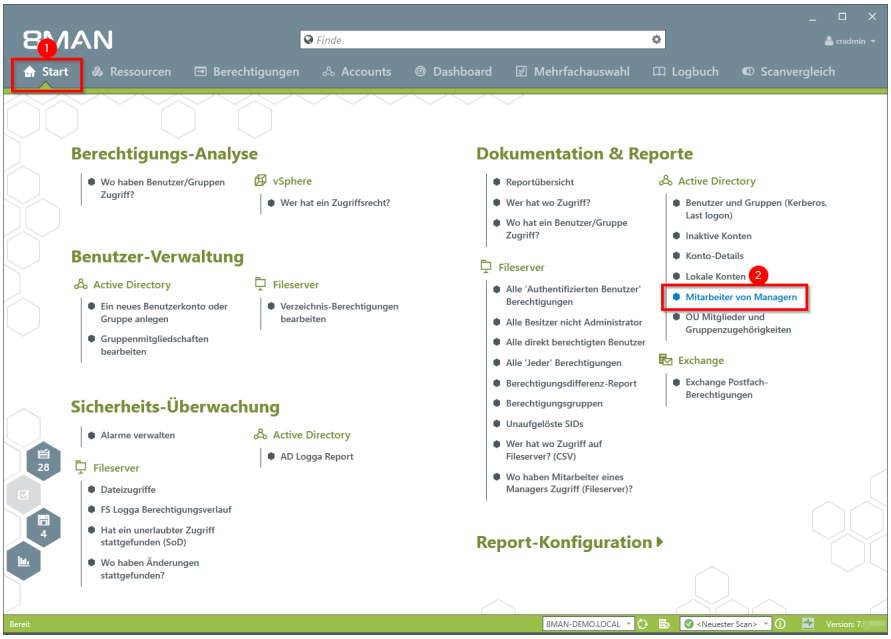
Der Report nutzt die im Active Directory unter dem Attribut "Manager" hinterlegten Informationen.

Weiterführende Services

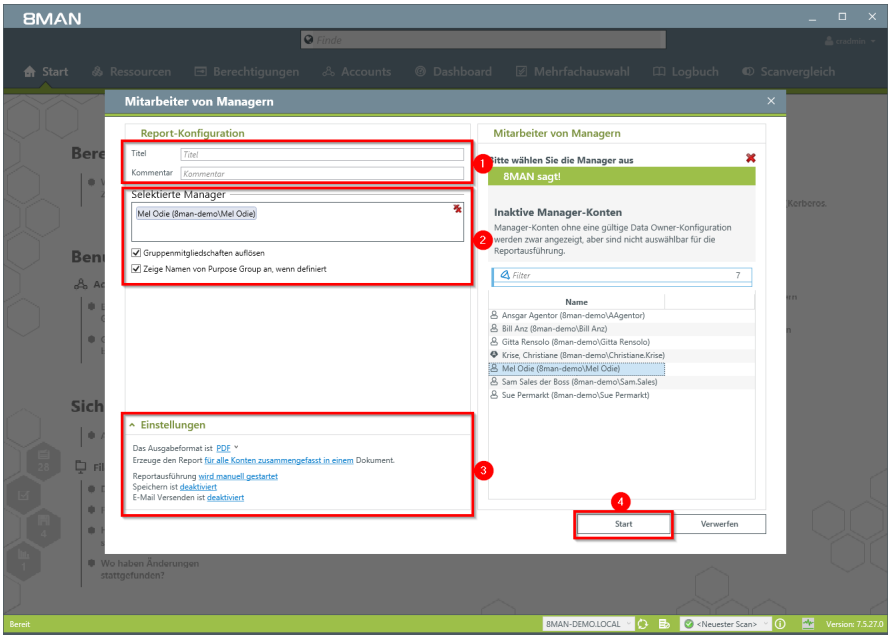
Für mehr Detailtiefe und der Einbeziehung zugewiesener Fileserver-Ressourcen empfehlen wir den Report:

Wo haben die Mitarbeiter eines Managers Zugriff?

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Mitarbeiter von Managern".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.2.2 Reporte für Administratoren

5.2.2.1 Konto-Details von Nutzern zeigen

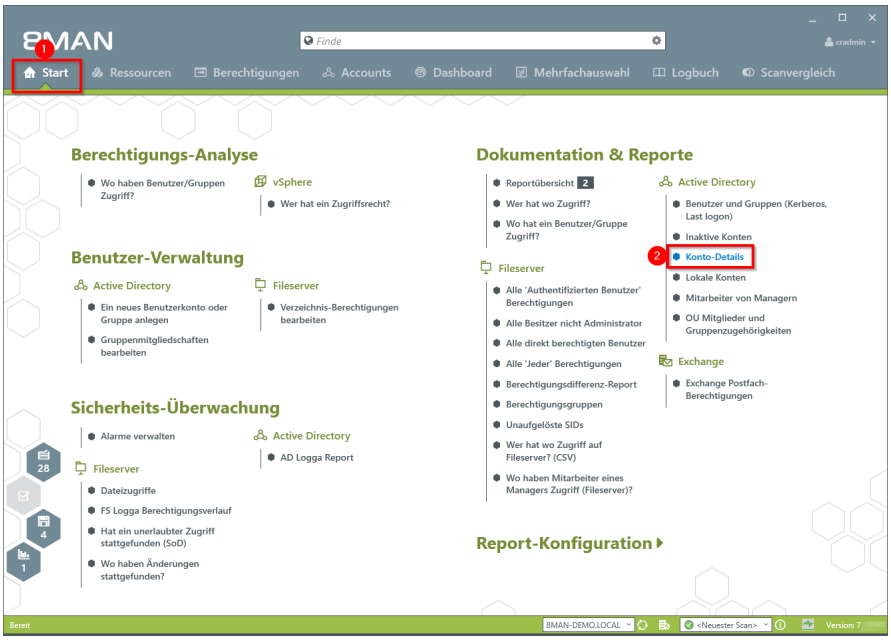
Hintergrund / Mehrwert

Die Erfassung der Kontodetails ist zentral für ein professionelles Active Directory Management. Folgende Informationen zeigt 8MAN in einem strukturierten Report:

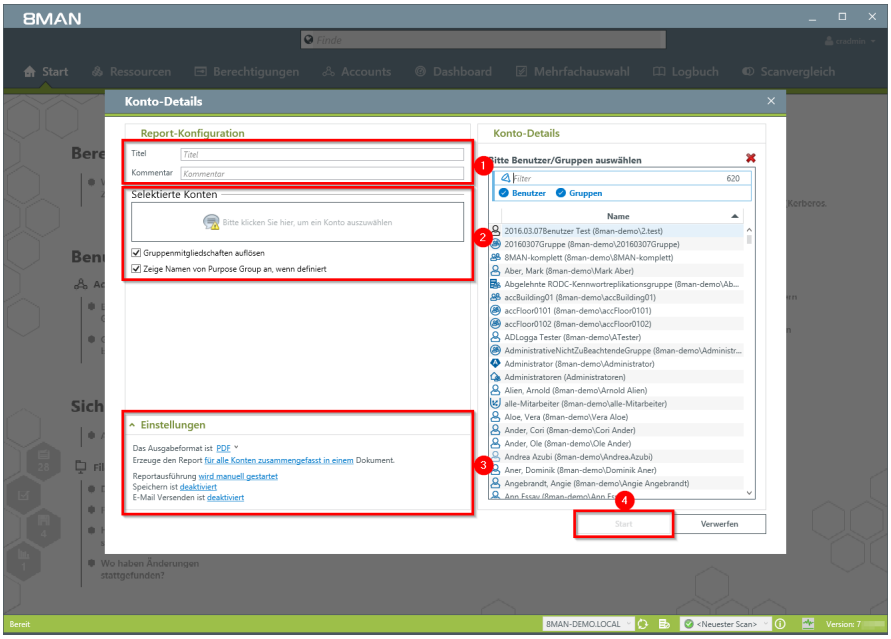
- Ablaufdatum des Kontos
- Anzeigename
- Benutzeranmeldename
- Common Name
- Definierter Name
- Email-Adresse
- LDAP ADsPath
- Letzte Anmeldung
- Objekt GUID
- Objekt SID
- SAM Account Name
- SAM Account Typ
- Gruppenmitgliedschaften
- Namen von Purpose Groups
- Eltern + Kinder

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.6 Vergabe von Zutrittsberechtigungen.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Konto-Details".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.2.2.2 Inaktive Konten (Benutzer oder Computer) finden

Hintergrund / Mehrwert

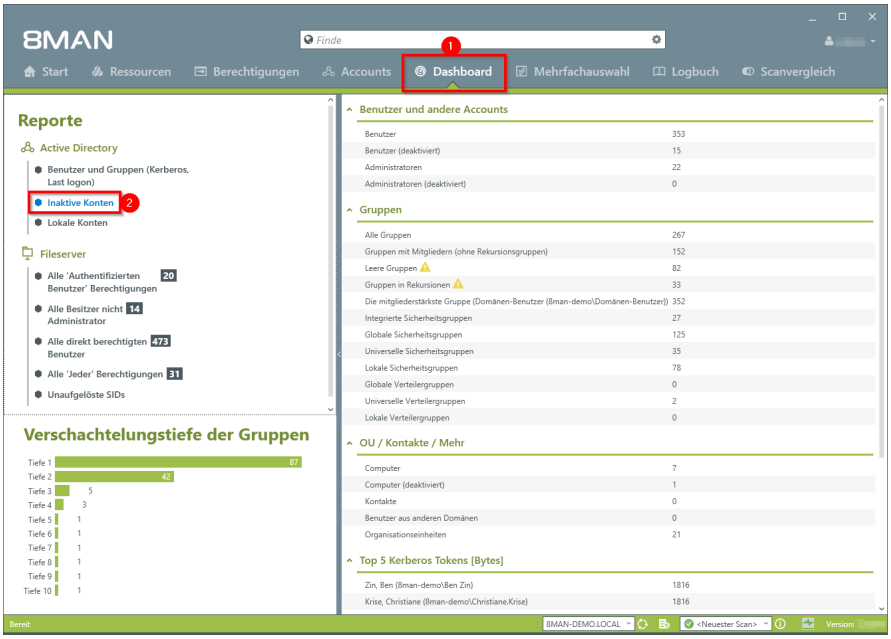
Inaktive Konten können unerkannt von Menschen oder Schadsoftware für Datendiebstahl und Manipulation genutzt werden. Oft sind Sie ein Indiz für eine gestörte Kommunikation zwischen der Personalabteilung und der IT, denn: Inaktive Nutzerkonten sind oft die Überbleibsel längst ausgeschiedener Mitarbeiter. 8MAN zeigt sämtliche inaktive Konten im Active Directory für Sie an. Löschen oder deaktivieren Sie die Konten, die keine Funktion mehr erfüllen.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 4.133 Geeignete Auswahl von Authentikationsmechanismen.

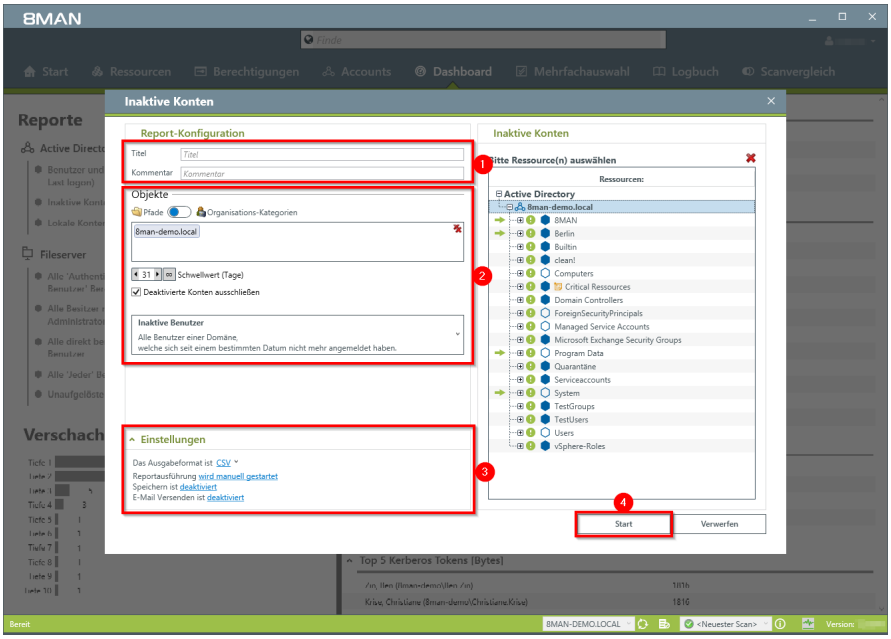
Weiterführende Services

Einen Nutzer und seine Berechtigungen löschen
Einen Nutzer mittels „Soft Delete“ löschen
Einen Nutzer deaktivieren
Inaktive Konten identifizieren (Webclient)
Konten im Bulk deaktivieren (Webclient)

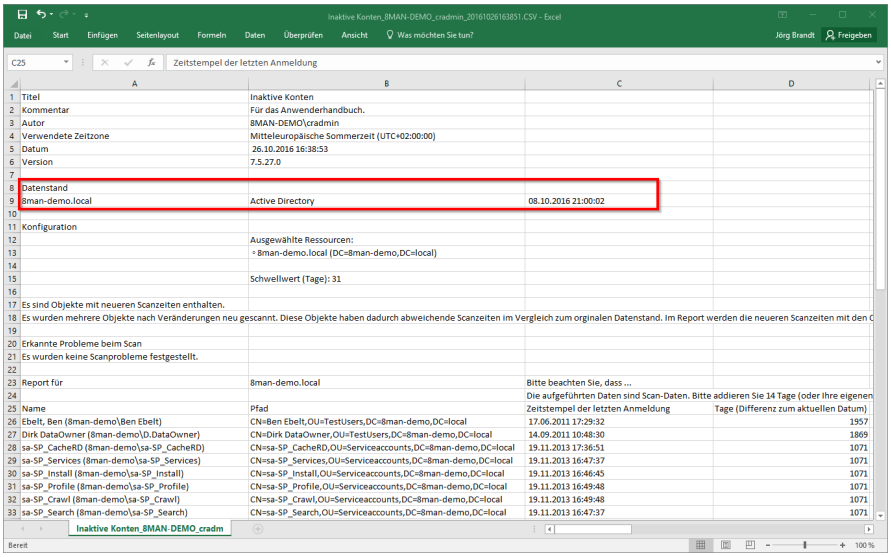
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Dashboard"*
2. *Klicken Sie auf "Inaktive Konten"*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports. Mit dem Schwellwert legen Sie fest, ab wie viel Tagen ein Konto als inaktiv gelten soll.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*



	A	B	C	D
1	Titel	Inaktive Konten		
2	Kommentar	Für das Anwenderhandbuch.		
3	Autor	8MAN-DEMO\cradmin		
4	Verwendete Zeitzone	Mitteleuropäische Sommerzeit (UTC+02:00:00)		
5	Datum	26.10.2016 16:38:53		
6	Version	7.5.27.0		
7				
8	Datenstand			
9	8man-demo.local	Active Directory	08.10.2016 21:00:02	
10				
11	Konfiguration			
12		Ausgewählte Ressourcen:		
13		◦ 8man-demo.local (DC=8man-demo,DC=local)		
14				
15		Schwellwert (Tage): 31		
16				
17	Es sind Objekte mit neueren Scanzeiten enthalten.			
18	Es wurden mehrere Objekte nach Veränderungen neu gescannt. Diese Objekte haben dadurch abweichende Scanzeiten im Vergleich zum orginalen Datenstand. Im Report werden die neueren Scanzeiten mit den C			
19				
20	Erkannte Probleme beim Scan			
21	Es wurden keine Scanprobleme festgestellt.			
22				
23	Report für	8man-demo.local	Bitte beachten Sie, dass ...	
24			Die aufgeführten Daten sind Scan-Daten. Bitte addieren Sie 14 Tage (oder Ihre eigenen	
25	Name	Pfad	Zeitstempel der letzten Anmeldung	Tage (Differenz zum aktuellen Datum)
26	Ebelt, Ben (8man-demo\Ben Ebelt)	CN=Ben Ebelt,OU=TestUsers,DC=8man-demo,DC=local	17.06.2011 17:29:32	1957
27	Dirk DataOwner (8man-demo\D.DataOwner)	CN=Dirk DataOwner,OU=TestUsers,DC=8man-demo,DC=local	14.09.2011 10:48:30	1869
28	sa-SP_CacheRD (8man-demo\sa-SP_CacheRD)	CN=sa-SP_CacheRD,OU=Serviceaccounts,DC=8man-demo,DC=local	19.11.2013 17:36:51	1071
29	sa-SP_Services (8man-demo\sa-SP_Services)	CN=sa-SP_Services,OU=Serviceaccounts,DC=8man-demo,DC=local	19.11.2013 16:47:37	1071
30	sa-SP_Install (8man-demo\sa-SP_Install)	CN=sa-SP_Install,OU=Serviceaccounts,DC=8man-demo,DC=local	19.11.2013 16:46:45	1071
31	sa-SP_Profile (8man-demo\sa-SP_Profile)	CN=sa-SP_Profile,OU=Serviceaccounts,DC=8man-demo,DC=local	19.11.2013 16:49:48	1071
32	sa-SP_Crawl (8man-demo\sa-SP_Crawl)	CN=sa-SP_Crawl,OU=Serviceaccounts,DC=8man-demo,DC=local	19.11.2013 16:49:48	1071
33	sa-SP_Search (8man-demo\sa-SP_Search)	CN=sa-SP_Search,OU=Serviceaccounts,DC=8man-demo,DC=local	19.11.2013 16:47:37	1071

Prüfen Sie im Report den verwendeten Datenstand. Bei älteren Scandaten treten Differenzen in den ermittelten Tagen seit dem letzten Login auf.

5.2.2.3 Report: OU Mitglieder und Gruppenzugehörigkeiten

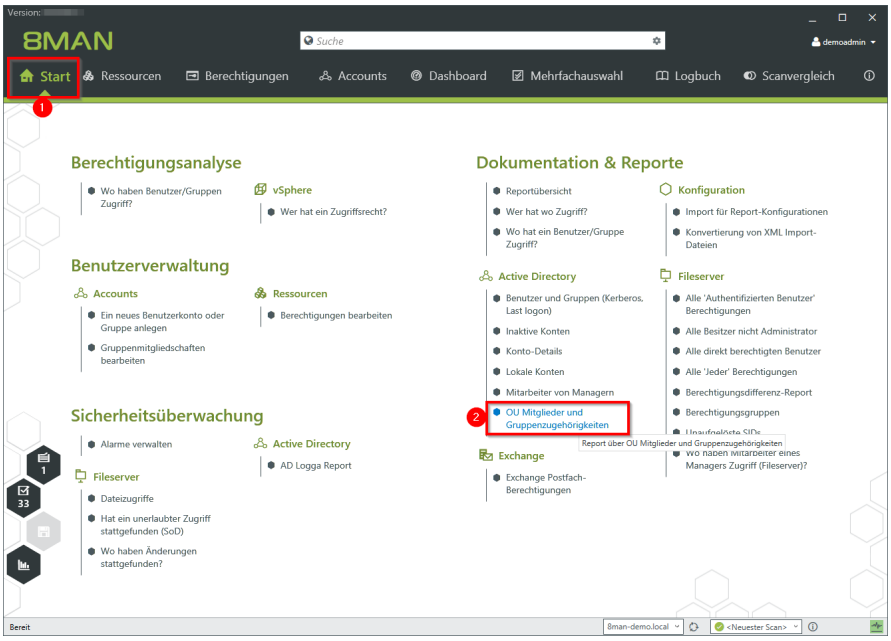
Hintergrund / Mehrwert

8MAN erlaubt eine schnelle Auswertung über die Gruppen und Benutzer, die sich in einer Organisational Unit (OU) befinden.

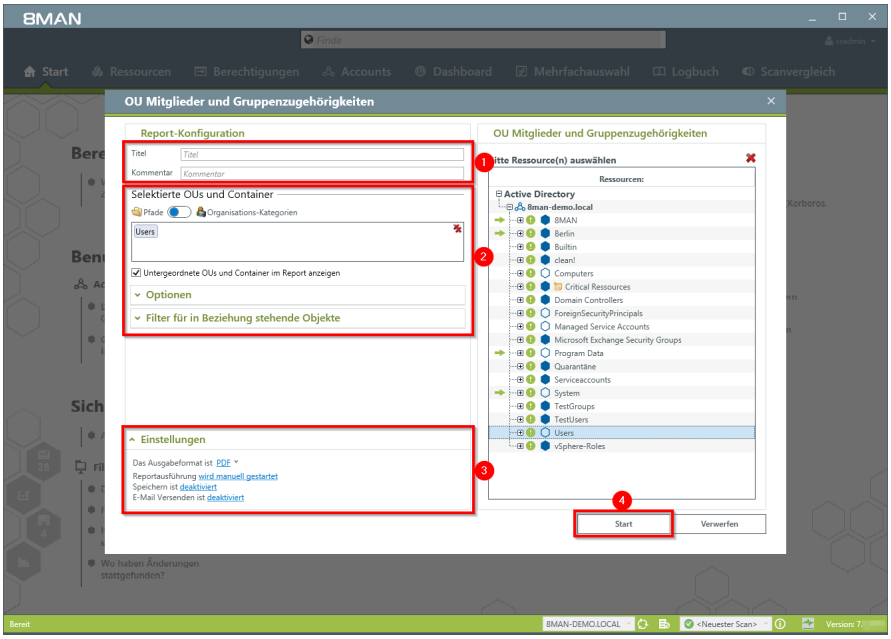
Dies gewährleistet, ausgehend von einer OU, die vorhandenen Gruppen und Nutzerkonten und deren Beziehung untereinander zu prüfen.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "OU Mitglieder und Gruppenzugehörigkeiten".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports und wählen Sie zwischen verschiedenen Layouts.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.2.2.4 Benutzer und Gruppen Report

Hintergrund / Mehrwert

Der Report Benutzer und Gruppen zeigt alle Benutzerkonten und Gruppen im AD und einige ihrer Merkmale und Attribute.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 4.133 Geeignete Auswahl von Authentikationsmechanismen.

Benutzerkonten

Zentral ist die Anzeige des Kerberos Tokens und des Last Logon Timestamp. Letztgenannter zeigt domainencontrollerübergreifend die letzte Anmeldung des AD Kontos im Netzwerk. Die Größe des Kerberos Token ist Ausdruck der Anzahl von Gruppenmitgliedschaften. Viele Gruppenmitgliedschaften indizieren möglich Überberechtigungen. Wird die Obergrenze von 64 KB überschritten, ist eine Anmeldung im Netzwerk nicht mehr möglich.

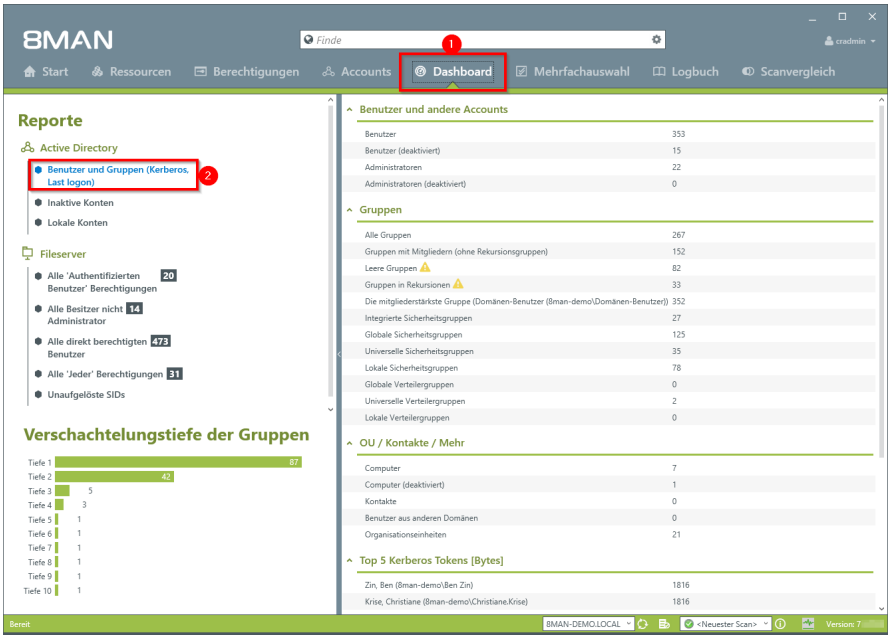
Darüber hinaus finden sich folgende Angaben:

- Kontoablaufdatum
- Kennwortablauf ja/nein
- Adminkonto ja/nein

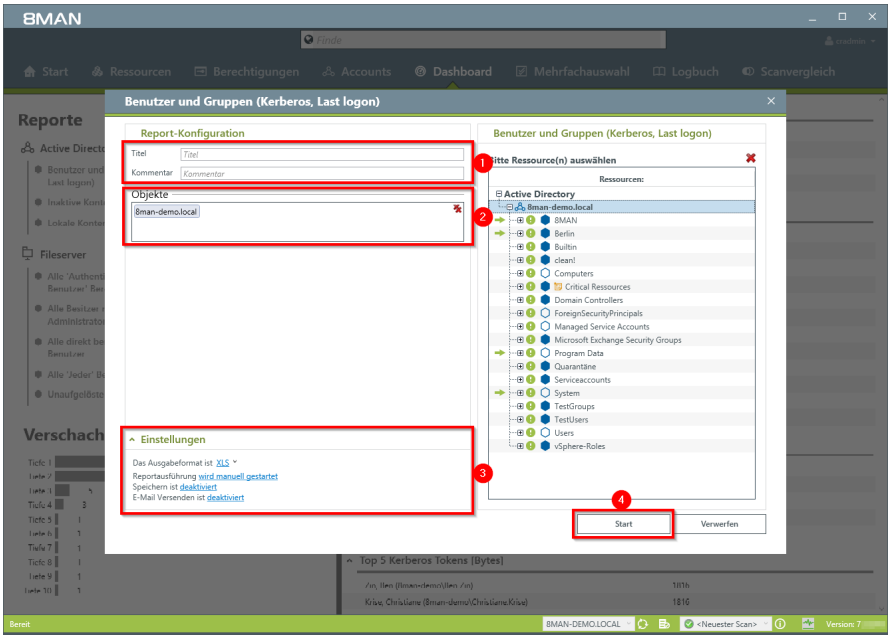
Gruppen:

Zeigt direkte und indirekte Gruppenmitgliedschaften sowie Gruppentyp (lokal, global, universell)

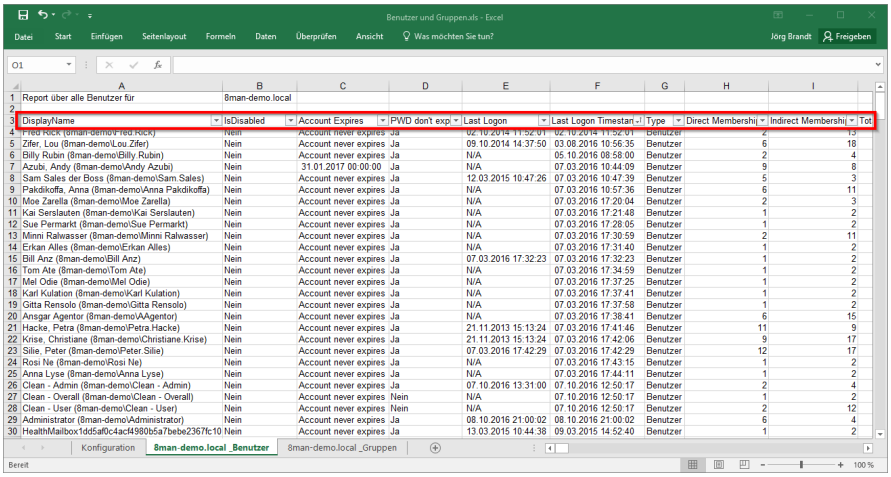
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Dashboard".*
2. *Klicken Sie auf "Benutzer und Gruppen".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*



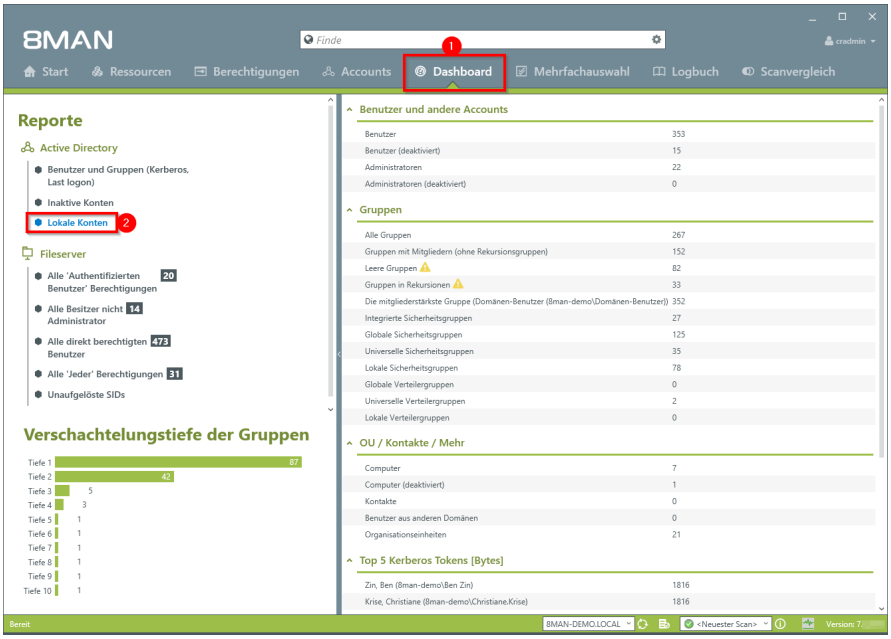
Öffnen Sie den Report in Excel und filtern die Daten nach Belieben.

5.2.2.5 Lokale Konten identifizieren

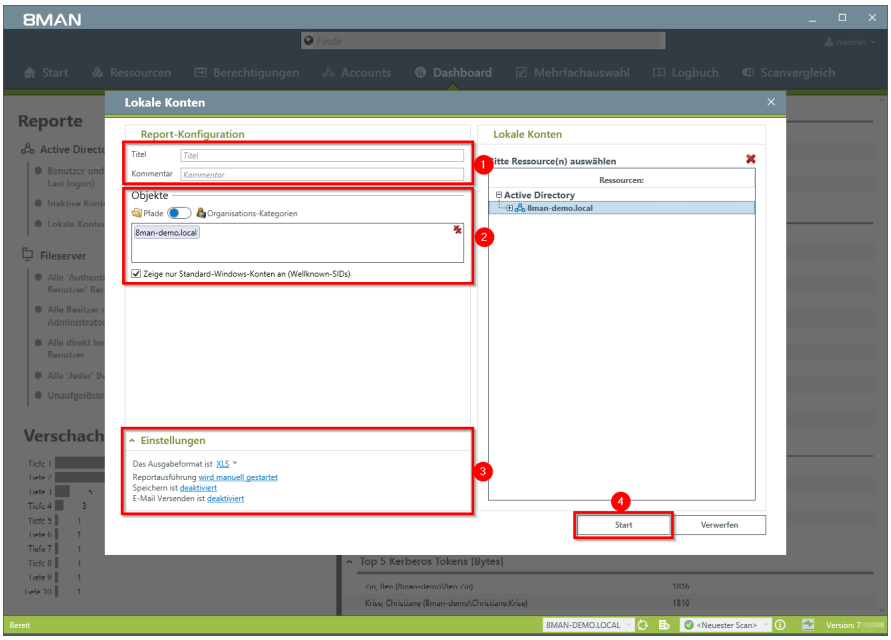
Hintergrund / Mehrwert

Der Lokale Konten Report zeigt lokale administrative Rechte auf Endgeräten an. Damit wird ersichtlich, welcher Administrator und welcher User auf welches Endgerät zugreifen kann. Auch hier gilt das "Principle of least privilege". Der Report schafft im Hinblick auf die Rechtesituation im Unternehmen ein vollständiges Bild. Denn: Lokale Konten Rechte sind über AD Mitgliedschaften nicht ersichtlich.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Dashboard".*
2. *Klicken Sie auf "Lokale Konten".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.2.3 Organisationshilfen für Administratoren

Neben der automatischen Dokumentation und der Reporte verfügt 8MAN über eine Reihe von Dokumentationsfeatures.

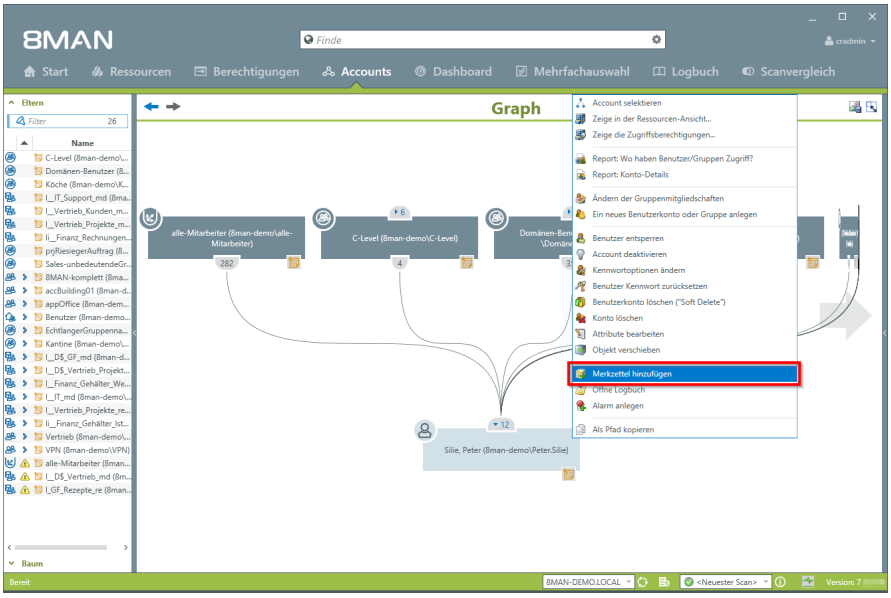
So können Sie im System händisch Post-its auf Objekte "kleben" oder AD Gruppen mit Klarnamen als "Purpose Groups" beschriften.

5.2.3.1 Notizen an Nutzerkonten und Gruppen heften

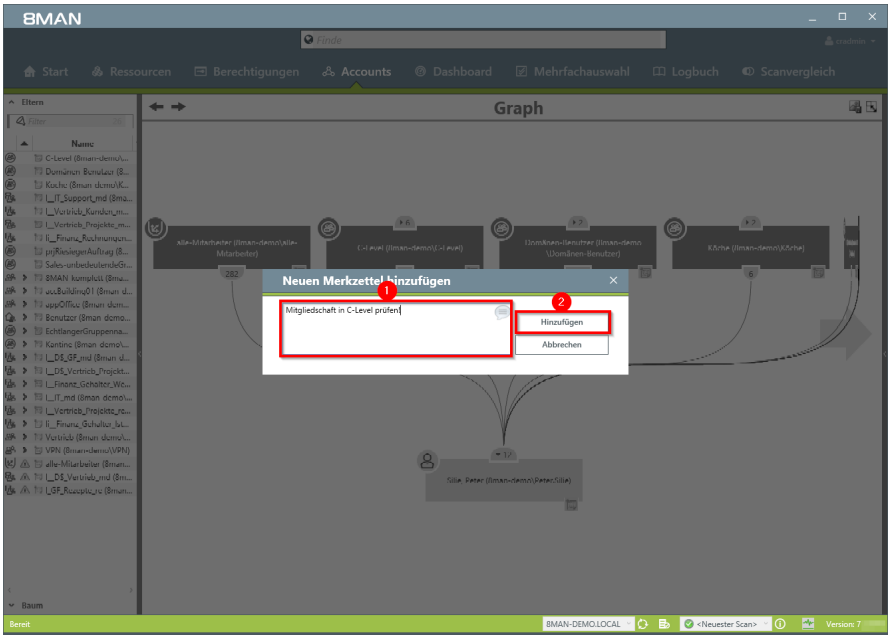
Hintergrund / Mehrwert

Markieren Sie Nutzerkonten und Gruppen mit Merkzetteln. Damit knüpfen Sie Aufgaben direkt an die Objekte.

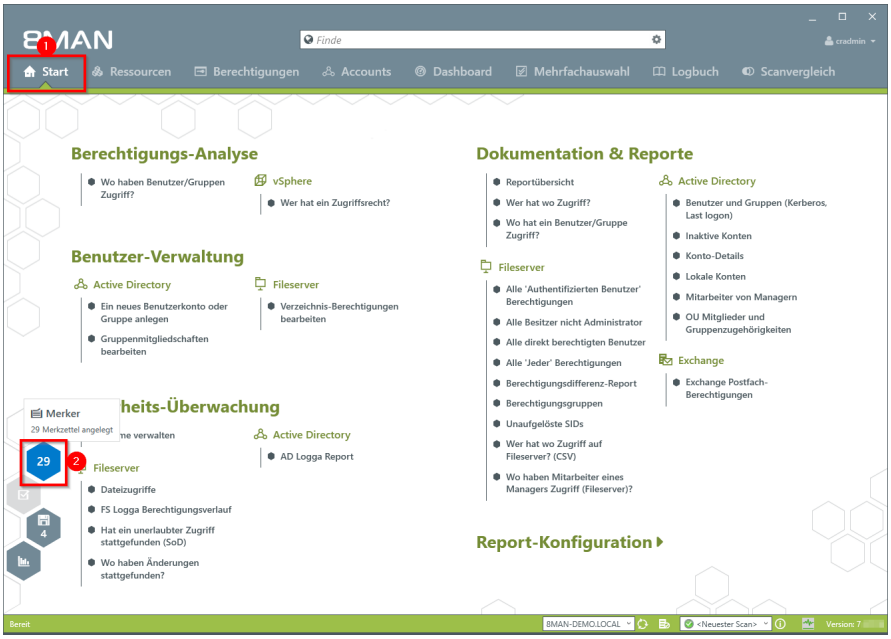
Der Prozess in einzelnen Schritten



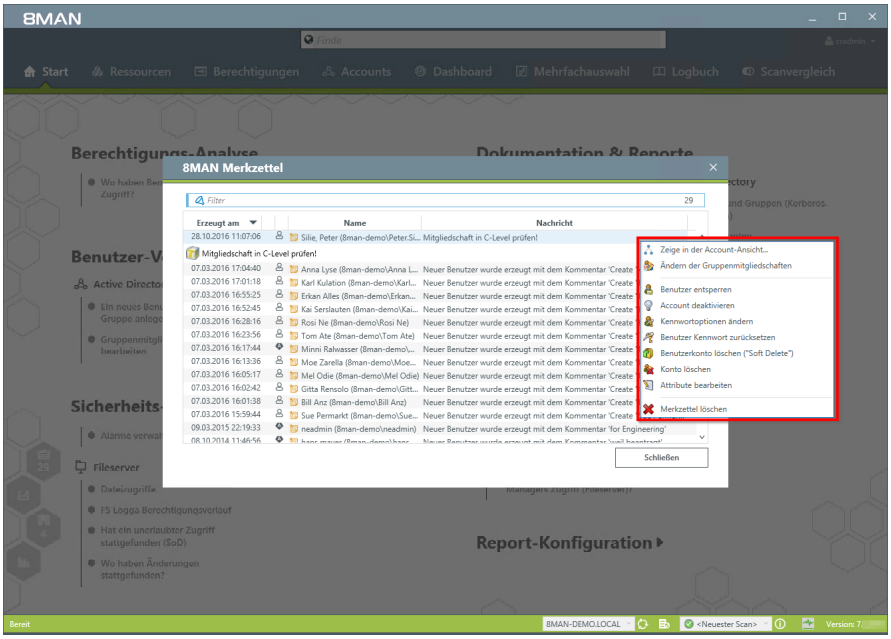
Rechtsklicken Sie auf ein Konto und wählen "Merkzettel hinzufügen" im Kontextmenü.



1. *Tragen Sie eine Notiz ein.*
2. *Klicken Sie auf "Hinzufügen".*



1. *Wählen Sie "Start".*
2. *Klicken Sie auf die Wabe, um zu Ihren Merkzetteln zu gelangen.*



In der Liste finden Sie Ihre Merkzettel. Mit Rechtklick starten Sie direkt verschiedene Aktionen.

5.2.3.2 Purpose Groups: Gruppen bezeichnen

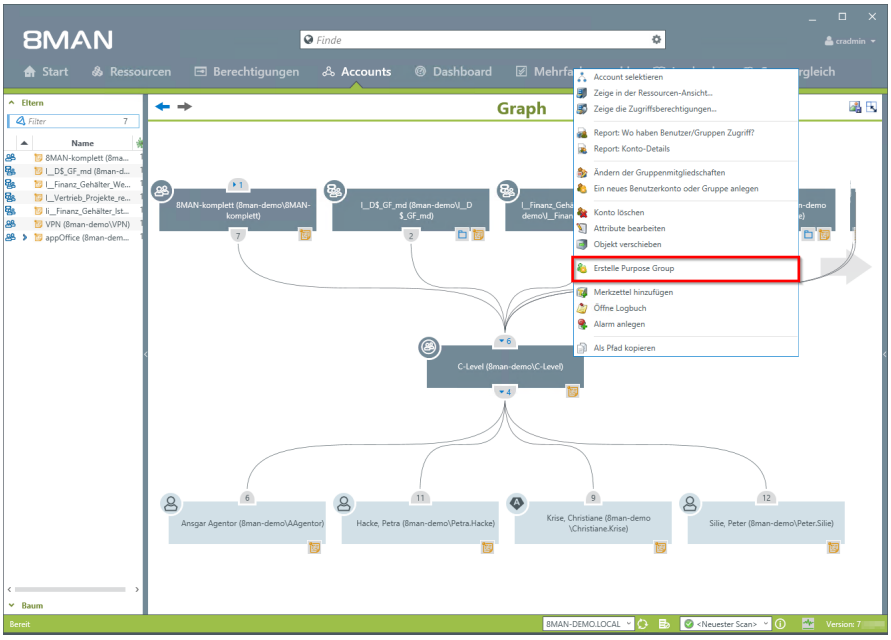
Hintergrund / Mehrwert

Purpose Groups schaffen klare Bezeichnungen für AD Gruppen. Diese haben im System technische Bezeichnungen und Administratoren können nicht schnell sehen, wozu sie dienen. Schaffen Sie Transparenz und vergeben Klarnamen.

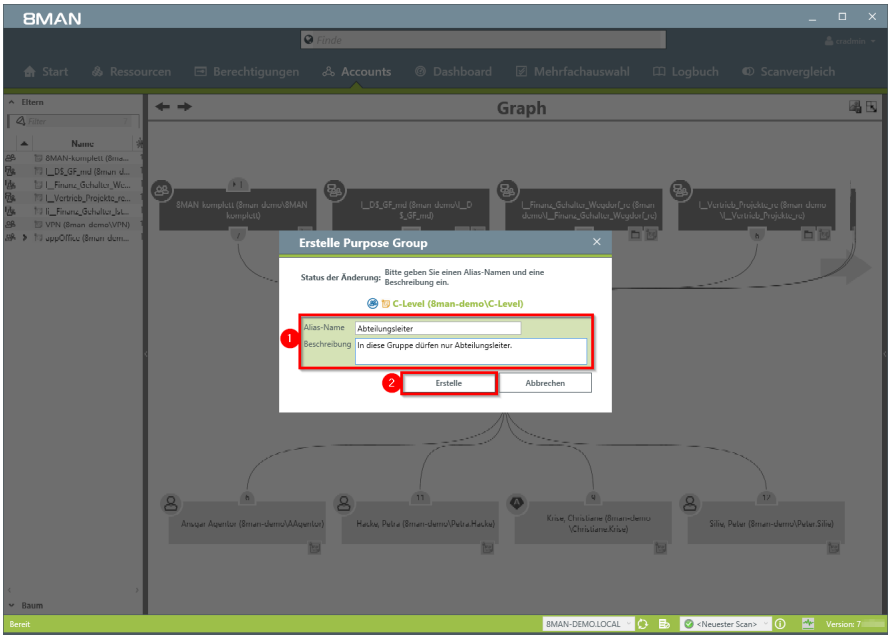
Die Bezeichnungen sind nur durch die 8MAN UI ersichtlich. Die tatsächliche Gruppenbezeichnung bleibt im Active Directory gleich.

5.2.3.2.1 Eine Purpose Group erstellen

Der Prozess in einzelnen Schritten



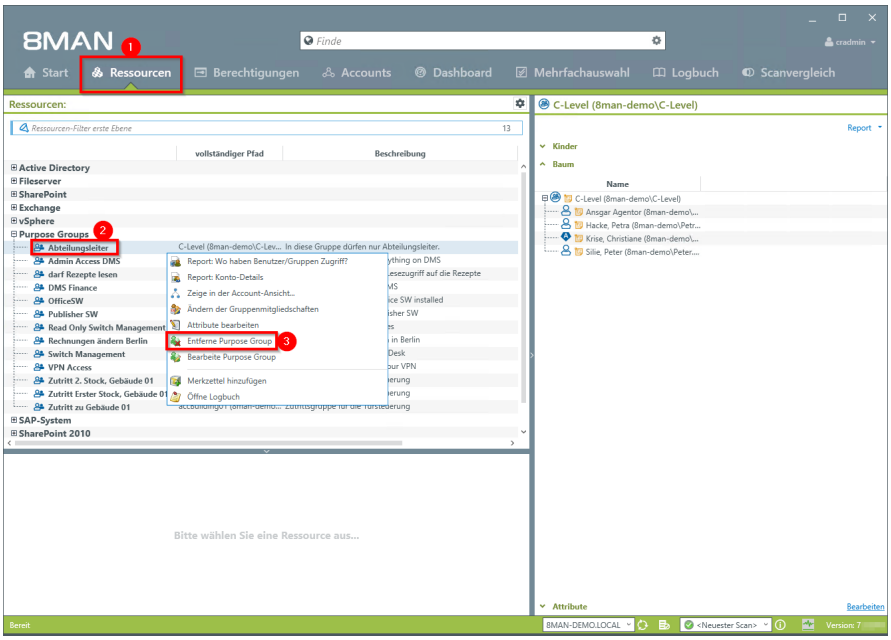
Klicken Sie auf eine AD Gruppe mit der rechten Maustaste. Wählen Sie "Erstelle Purpose Group" im Kontext Menü.



1. *Vergeben Sie einen Alias-Namen und hinterlegen Sie eine Beschreibung der Gruppe.*
2. *Klicken Sie auf "Erstellen".*

5.2.3.2.2 Eine Purpose Group ändern oder löschen

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen"*
2. *Selektieren Sie die gewünschte Purpose Group mit Rechtsklick.*
3. *Klicken Sie im Kontextmenü auf "Entferne Purpose Group" oder auf "Bearbeite Purpose Group".*

Der Löschvorgang betrifft nur die Purpose Group, also die in 8MAN zugewiesene Bezeichnung. Im Active Directory ändert sich nichts.

5.3 Fileserver

5.3.1 Reporte für Führungskräfte

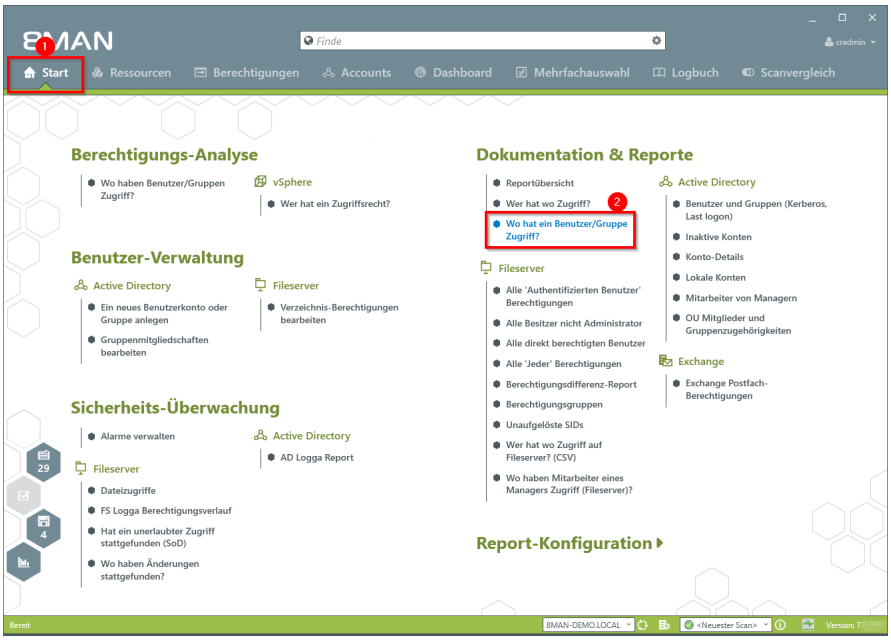
5.3.1.1 Wo haben Benutzer/Gruppen Zugriff? / Fokus Mitarbeiter

Hintergrund / Mehrwert

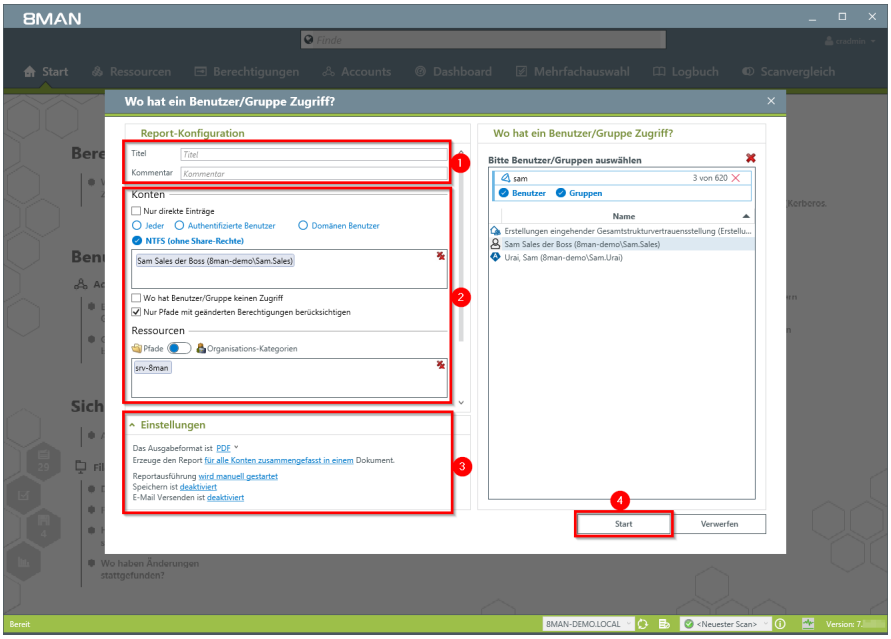
Der Report "Wo hat ein Benutzer/Gruppe Zugriff?" listet die Zugriffsrechte von Nutzerkonten und Gruppen auf ausgewählten Fileserver-Verzeichnissen in einem Dokument auf.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle, M 2.8 Vergabe von Zugriffsrechten sowie M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start"*
2. *Klicken Sie auf "Wo hat eine Benutzer/Gruppe" Zugriff?*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.3.1.2 Wer hat wo Zugriff? / Fokus Ressource

Hintergrund / Mehrwert

Führungskräfte wissen am besten, wer worauf Zugriff haben sollte. Insbesondere für sensible Fileserververzeichnisse muss vollständig Transparenz bestehen. Der Report "Wer hat wo Zugriff?" bietet eine vollständige Übersicht über alle Rechte (z. B. "Lesen" und "Schreiben") und Personen, die diese Rechte auf dem Verzeichnis ausüben können.

Der Report gibt der verantwortlichen Führungskraft eine Entscheidungsgrundlage, um zwei zentrale Fragen zu beantworten:

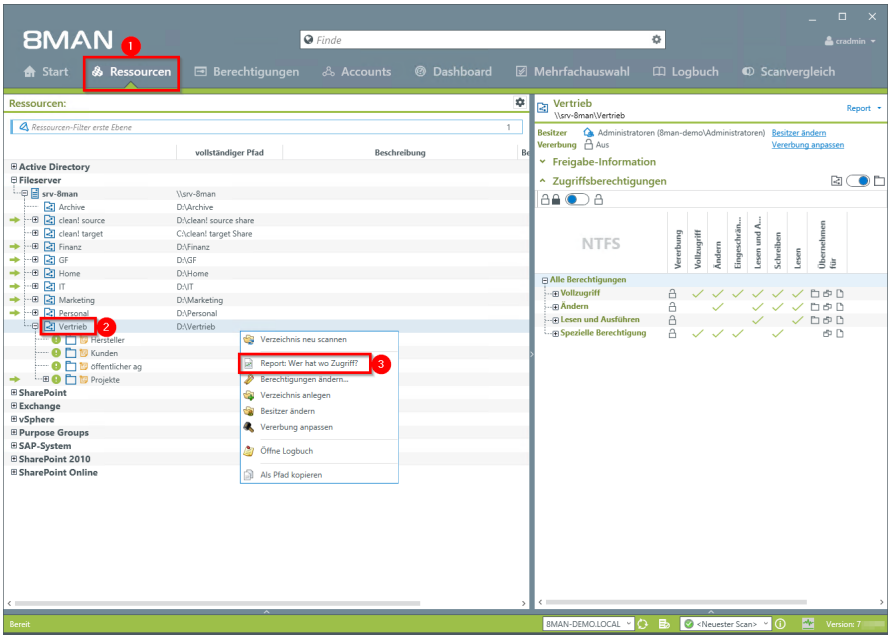
- Wer sollte Zugriff haben? (Erhöhung der Datensicherheit)
- Welche Zugriffsrechte sollten bestehen? (Erhöhung von Datenintegrität)

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.8 Vergabe von Zugriffsrechten sowie M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile.

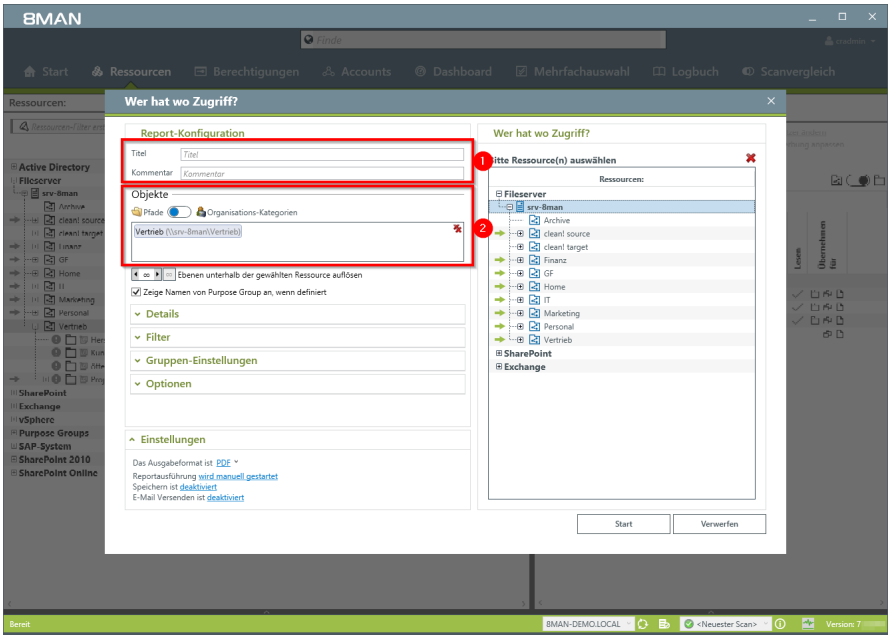
Weiterführende Services

Verzeichnisberechtigungen ändern

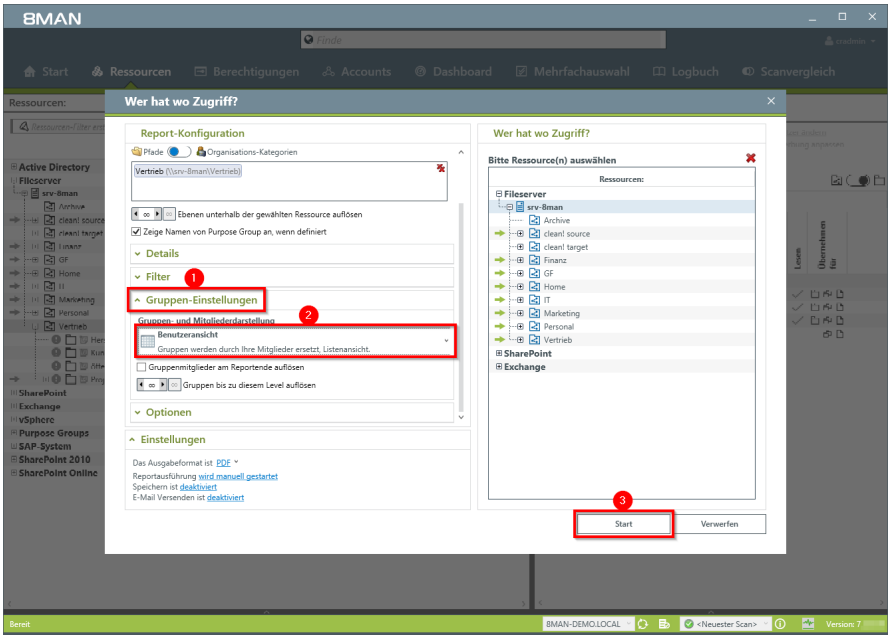
Der Prozess in einzelnen Schritten



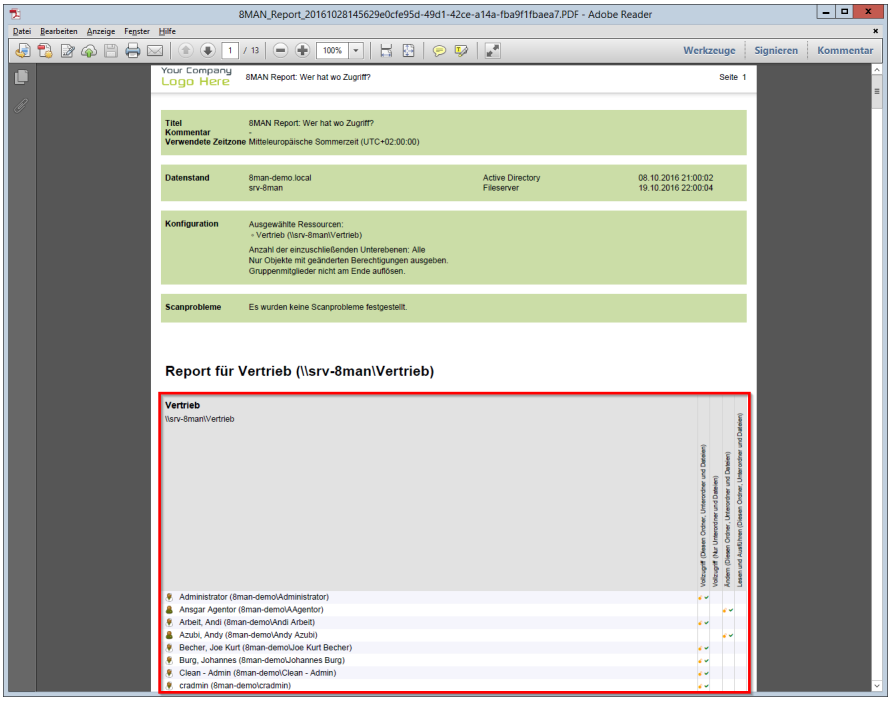
1. *Wählen Sie "Ressourcen".*
2. *Selektieren Sie mit Rechtsklick ein Verzeichnis, für das Sie verantwortlich sind.*
3. *Klicken Sie im Kontextmenü auf "Report: Wer hat wo Zugriff?".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Das eben gewählte Verzeichnis ist automatisch Teil der Objekte, die untersucht werden sollen. Sie können weitere Ressourcen hinzufügen.*



1. *Klappen Sie "Gruppen-Einstellungen" auf.*
2. *Zur Komplexitätsreduktion empfehlen wir "Benutzeransicht" zu wählen. Die restlichen Einstellungen richten sich an Experten.*
3. *Starten Sie die Reporterstellung.*



Prüfen Sie, ob die aufgelisteten Nutzer Zugriff haben sollten. Im zweiten Schritt sollten Sie prüfen, ob es für einige Nutzer nicht reicht, die Rechte von "Vollzugriff" auf "Lesen und Ausführen" herabzusetzen. Damit erreichen Sie eine höhere Datenintegrität.

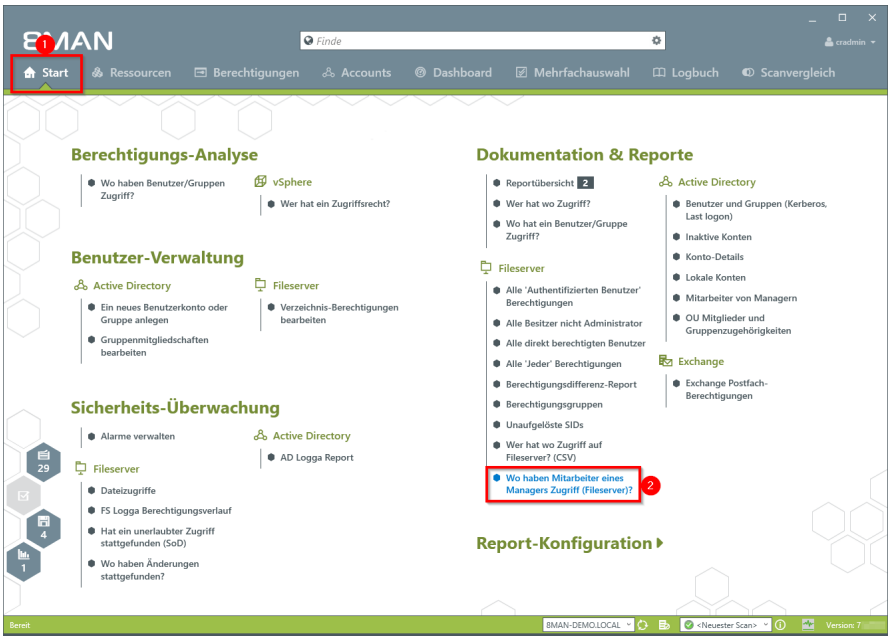
5.3.1.3 Wo haben Mitarbeiter eines Managers Zugriff?

Hintergrund / Mehrwert

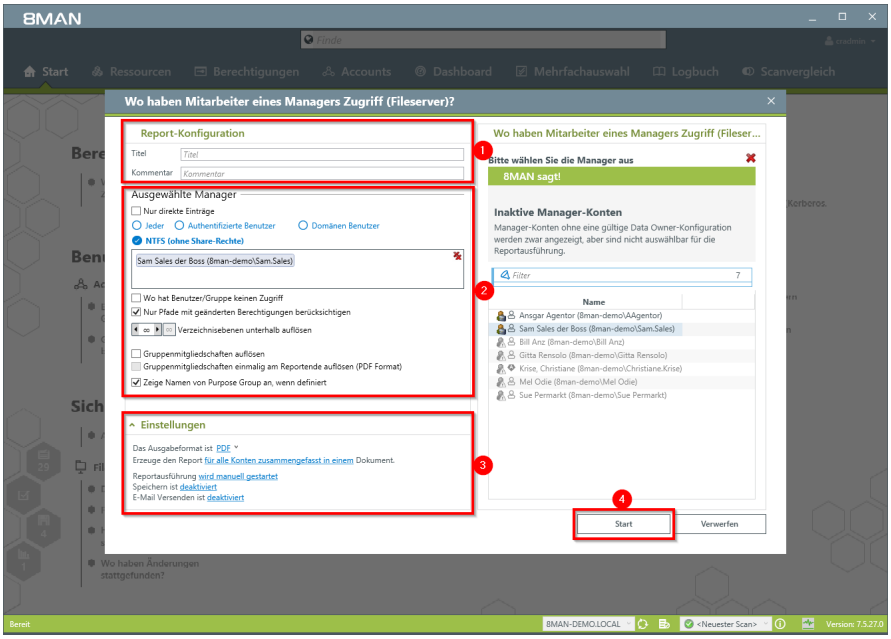
8MAN verfügt über einen speziellen Data Owner Report für Fileserver. Darin werden die im Active Directory hinterlegten Mitarbeiter (Attribut "Manager") mit den in der Data Owner Konfiguration hinterlegten Ressourcen zueinander in Beziehung gesetzt.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.8 Vergabe von Zugriffsrechten sowie M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Mitarbeiter von Managern".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports. Sie können nur Benutzer hinzufügen, bei denen das Manager-Attribut gesetzt ist und die eine gültige Data Owner Konfiguration haben.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.3.2 Reporte für Administratoren

5.3.2.1 „Jeder“ Berechtigungen identifizieren

Hintergrund / Mehrwert

Werden "Jeder-Konten" für die Vergabe von Berechtigungen benutzt, hat (fast) jeder Zugriff auf verknüpften Ressourcen. Die Folge ist eine massive Überberechtigung, also eine hohe Chance für unberechtigte Zugriffe.

8MAN zeigt Ihnen die Berechtigungen der "Jeder Accounts". Sie widersprechen dem "Principle of least Privilege" und sollten deshalb nicht verwendet werden.

Ein automatisches Entfernen von Jeder Berechtigungen ist möglich. Bevor Sie die Berechtigungen entfernen, sollten Sie den entsprechenden Ressourcen spezifische Gruppenberechtigungen zuweisen.

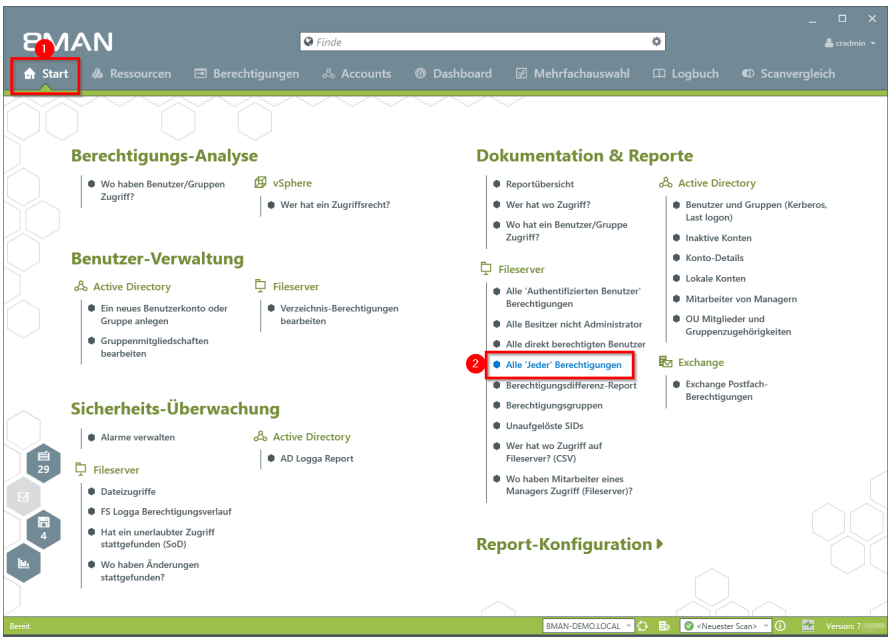
Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 4.247 Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista.

Weiterführende Services

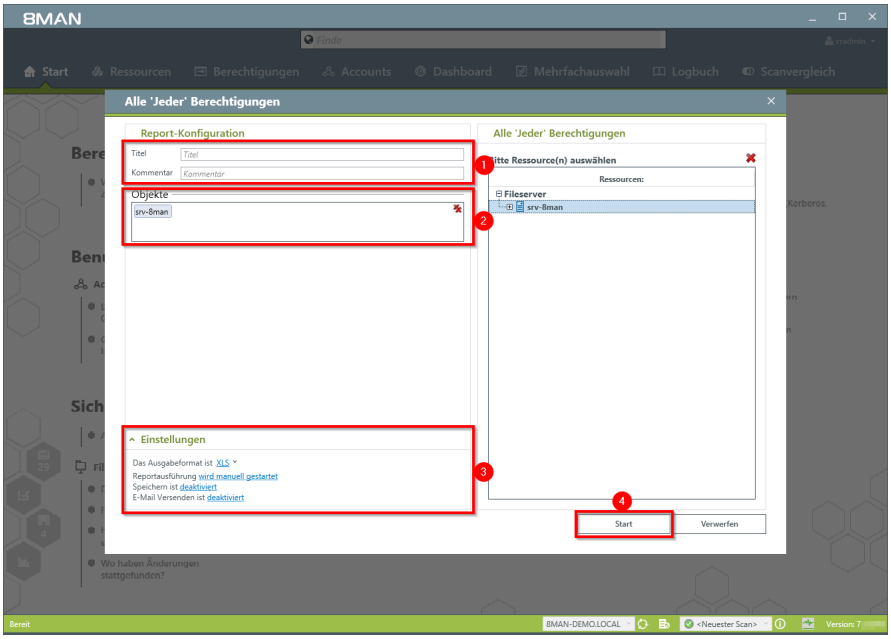
Behalten Sie ebenfalls die sicherheitskritisch brisanten "Authentifizierte Benutzer" im Blick.

Im Webclient identifizieren Sie global zugängliche Verzeichnisse oder entfernen Jeder-Berechtigungen im Bulk.

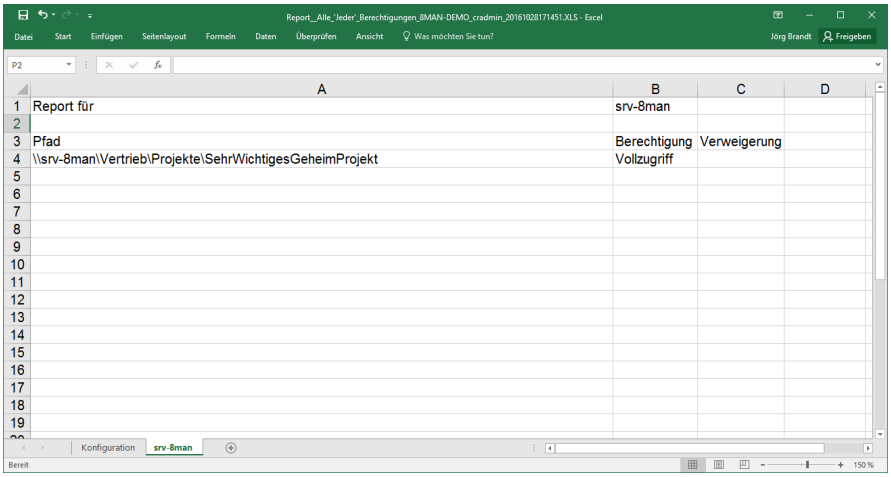
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Alle Jeder Berechtigungen".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*



	A	B	C	D
1	Report für	srv-8man		
2				
3	Pfad	Berechtigung	Verweigerung	
4	\\srv-8man\Vertrieb\Projekte\SehrWichtigesGeheimProjekt	Vollzugriff		

Im Beispielreport sehen Sie illustrativ ein geheimes Verzeichnis, auf das jeder zugreifen kann.

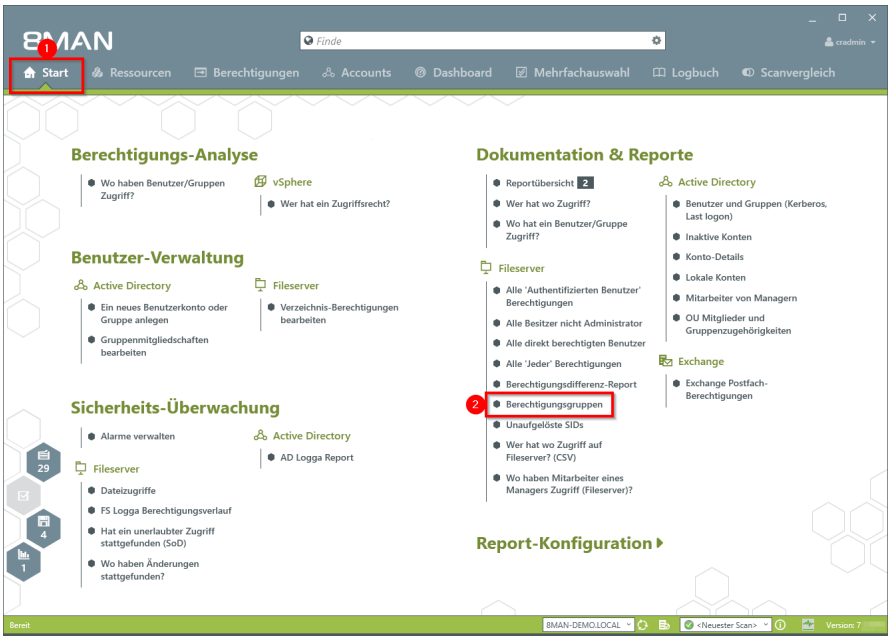
5.3.2.2 Wer kann wo über welche Berechtigungsgruppen zugreifen?

Hintergrund / Mehrwert

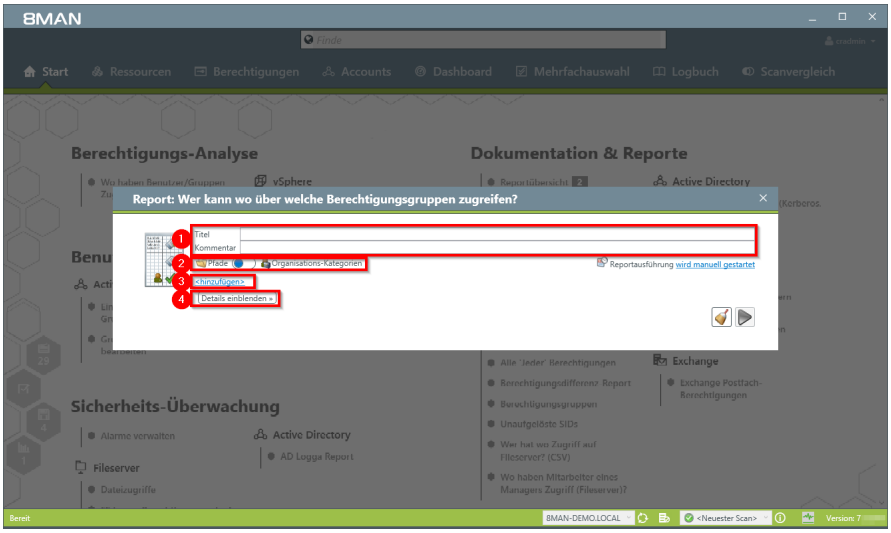
Der Report "Wer kann wo über welche Berechtigungsgruppe zugreifen?" zeigt die Berechtigungsgruppen auf von Ihnen ausgewählte Ressourcen und die Mitglieder, die dadurch Zugriff erhalten. Sie können statt einzelner Verzeichnispfade auch die von Ihnen in der Data Owner Konfiguration hinterlegten Organisations-Kategorien analysieren.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.8 Vergabe von Zugriffsrechten sowie M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile.

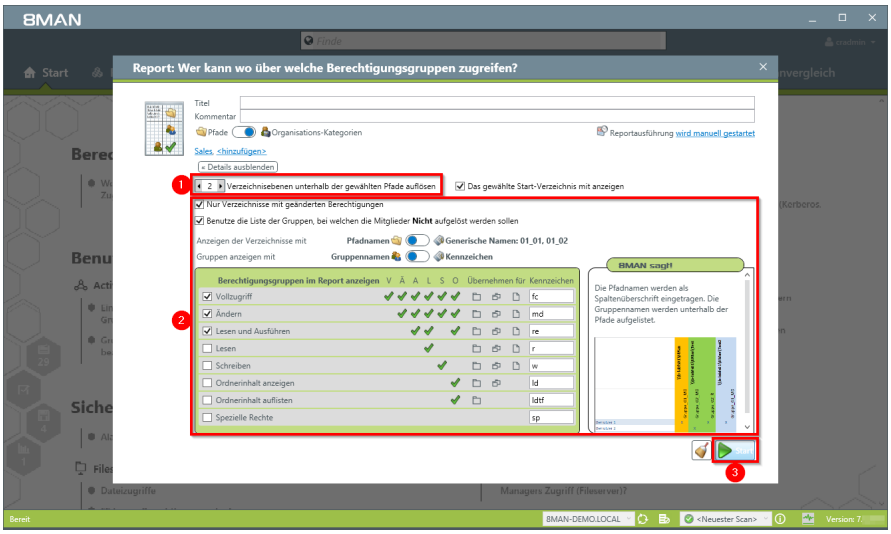
Der Prozess in einzelnen Schritten



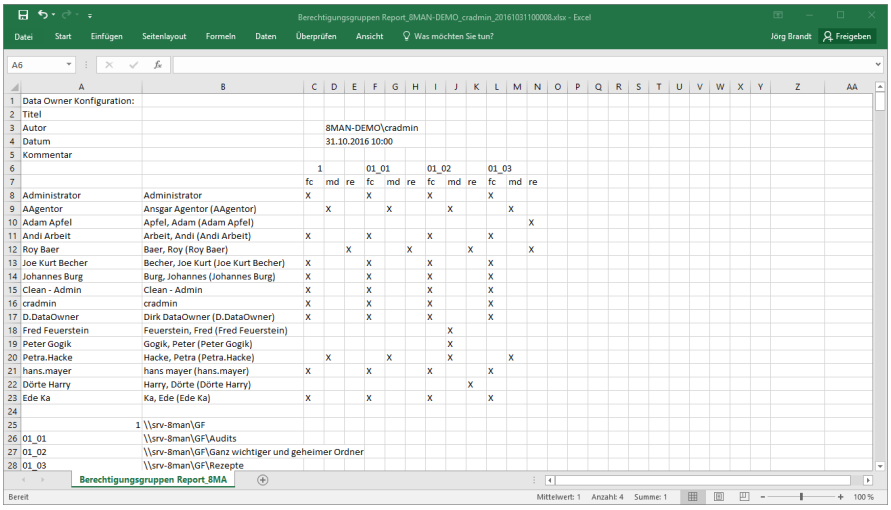
1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Berechtigungsgruppen".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Legen Sie fest, ob Sie den Umfang des Reports nach Verzeichnispfaden oder Organisationskategorien aus der Data Owner Konfiguration bestimmen wollen.*
3. *Definieren Sie den Umfang des Reports.*
4. *Klicken Sie auf "Details einblenden".*



1. *Um den Report kurz und damit aussagekräftig zu halten, empfehlen wir für die Verzeichnisebene einen geringen Wert zu wählen.*
2. *Konkretisieren Sie die im Report vorhandenen Inhalte weiter und legen verschiedene Layoutoptionen fest.*
3. *Starten Sie die Erstellung des Reports.*



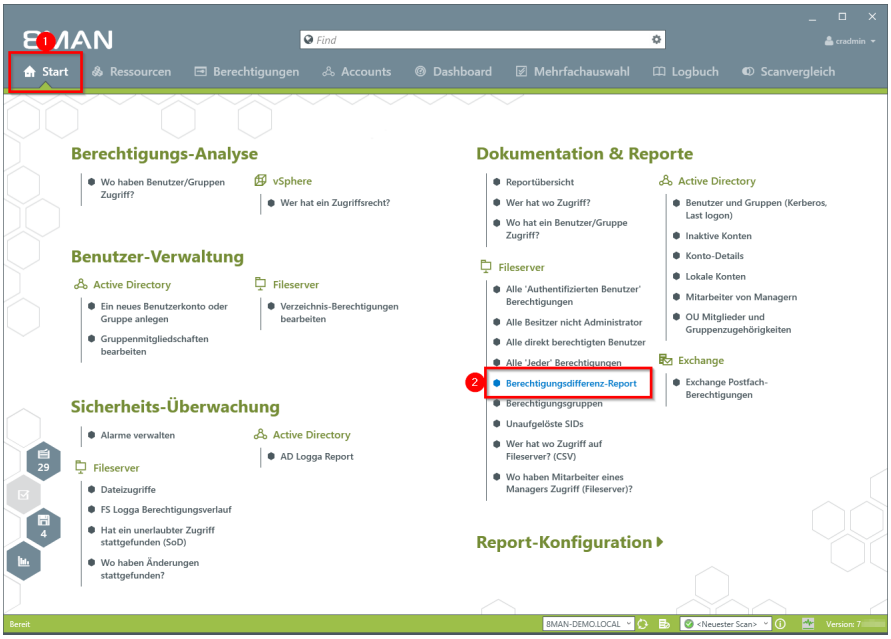
Sie erhalten eine Auflistung aller Nutzerkonten und Fileserverpfade und die entsprechenden Berechtigungsgruppen.

5.3.2.3 Berechtigungsdifferenz-Report

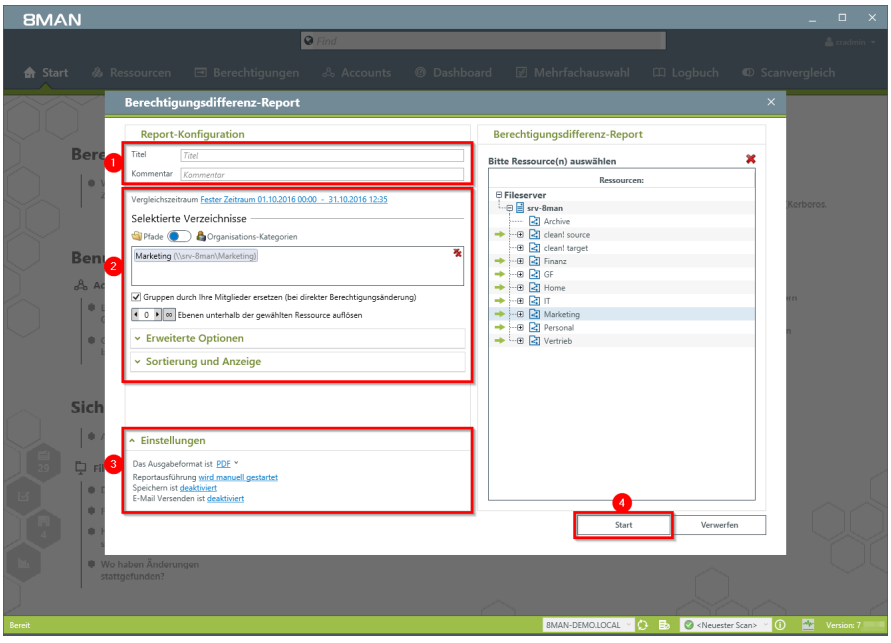
Hintergrund / Mehrwert

Der Berechtigungsdifferenz-Report zeigt die IST-Zustände von zwei Berechtigungssituationen auf dem Fileserver und vergleicht diese miteinander. Sie können somit feststellen, inwieweit sich Ihr Fileserver verändert hat.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Berechtigungsdifferenz-Report".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports, u. a. auch den Vergleichszeitraum.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.3.2.4 Verwaiste SIDs identifizieren

Hintergrund / Mehrwert

SIDs (Security Identifier) sind Zeichenfolgen, die einen Benutzer oder eine Gruppe eindeutig identifizieren. Werden direkt berechtigte Benutzer oder Gruppen im AD gelöscht, bleiben verwaiste SIDs im Dateisystem bestehen.

Mit Hilfe der verwaisten SID können Innentäter sich Zugriff auf Ressourcen verschaffen.

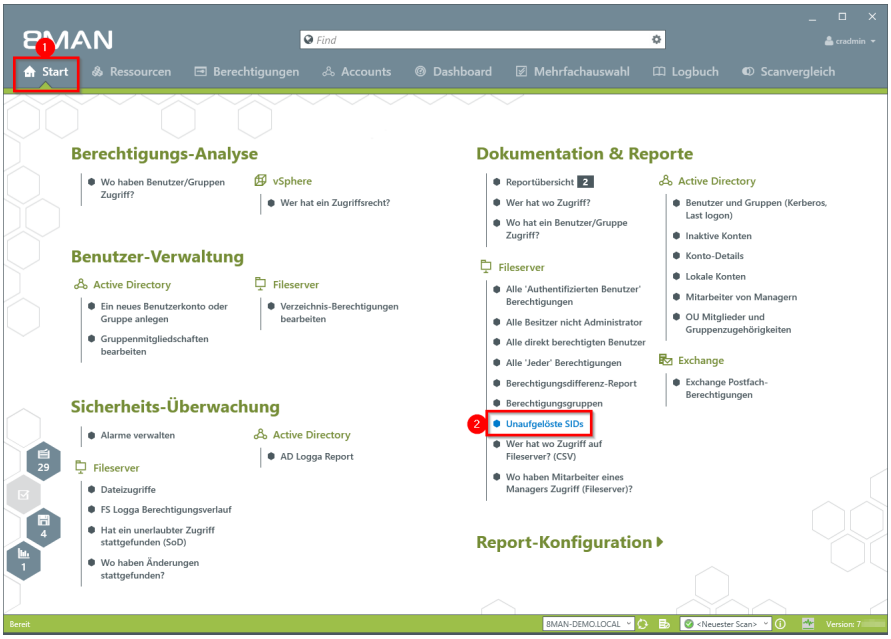
8MAN identifiziert verwaiste SIDs in Ihrem System. Diese können Sie im Anschluss löschen.

Weiterführende Services

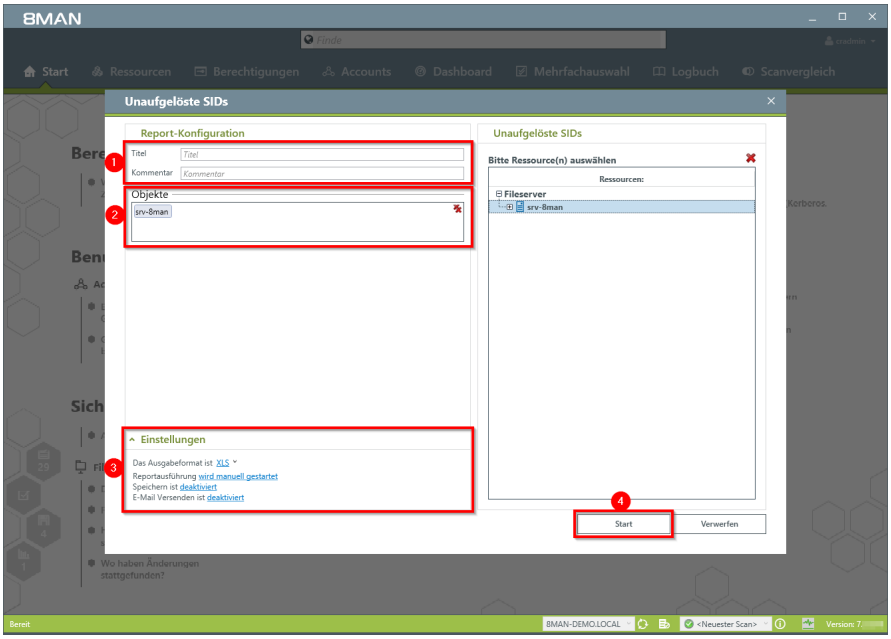
Verwaiste SIDs identifizieren und löschen (einzeln im rich client)

Verwaiste SIDs im Bulk löschen (Webclient)

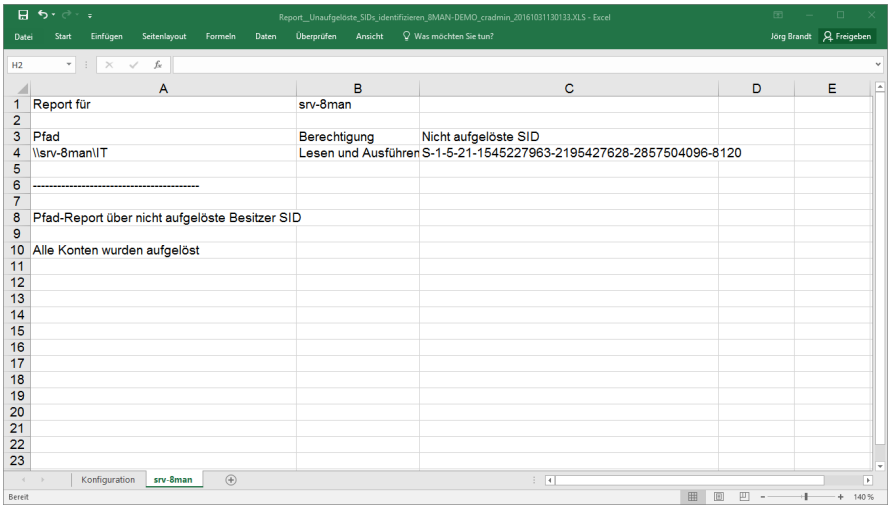
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Unaufgelöste SIDs".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*



Öffnen Sie den Report in Excel. Im Beispiel wurde für das Verzeichnis "IT" eine unaufgelöste SID identifiziert.

5.3.2.5 Direktberechtigungen identifizieren

Hintergrund / Mehrwert

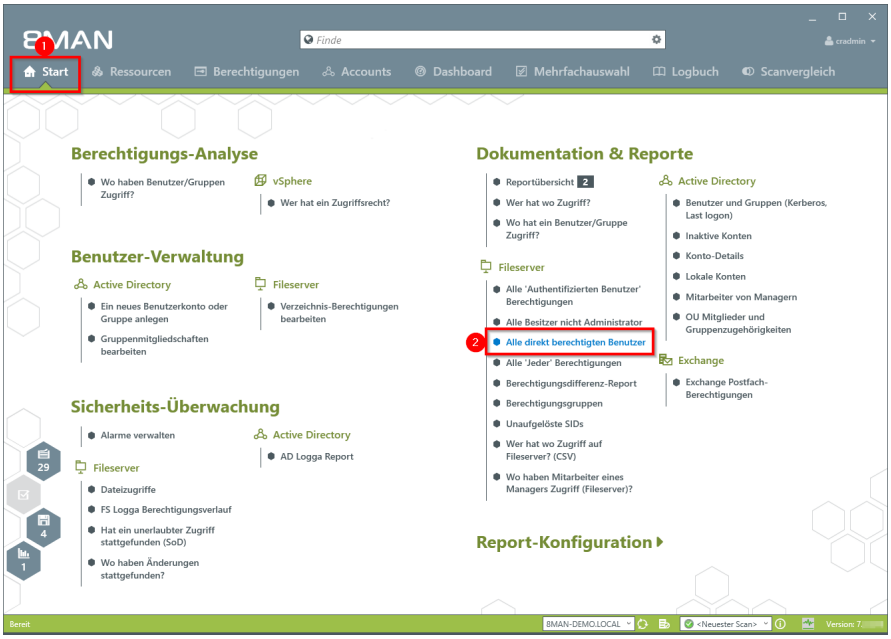
Direktberechtigungen sollten unter allen Umständen vermieden werden und durch Berechtigungen über Gruppen ersetzt werden. Direktberechtigungen sind ineffizient, weil jeder Nutzer einzeln berechtig werden muss. Darüber hinaus muss jedes Verzeichnis bei der Rechteentfernung gesondert geprüft werden. 8MAN zeigt Ihnen alle Direktberechtigungen auf Ihren Fileservern.

8MAN handelt strikt nach Microsoft Best Practice und legt für jede Berechtigung eine Gruppe an.

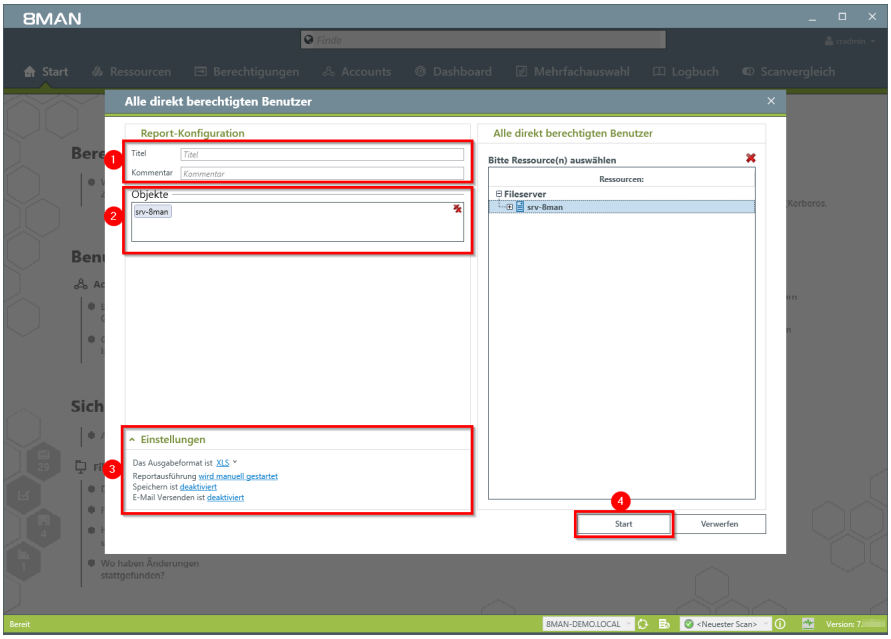
Weiterführende Services

Mit 8MAN Enterprise entfernen Sie einzelne Direktberechtigungen.
Mit Analyze & Act entfernen Sie Direktberechtigungen im Bulk (Webclient).

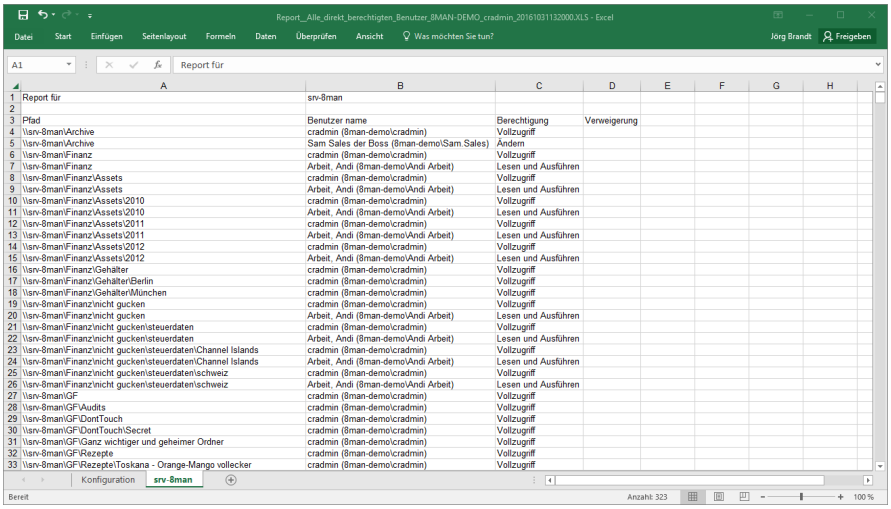
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Alle direkt berechtigten Benutzer".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*



	A	B	C	D
1	Report für	srv-8man		
2				
3	Pfad	Benutzer name	Berechtigung	Verweigerung
4	\\srv-8man\Archive	cradmin (8man-demo\cradmin)	Vollzugriff	
5	\\srv-8man\Archive	Sam Sales der Boss (8man-demo\Sam.Sales)	Ändern	
6	\\srv-8man\Finanz	cradmin (8man-demo\cradmin)	Vollzugriff	
7	\\srv-8man\Finanz	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
8	\\srv-8man\Finanz\Assets	cradmin (8man-demo\cradmin)	Vollzugriff	
9	\\srv-8man\Finanz\Assets	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
10	\\srv-8man\Finanz\Assets\2010	cradmin (8man-demo\cradmin)	Vollzugriff	
11	\\srv-8man\Finanz\Assets\2010	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
12	\\srv-8man\Finanz\Assets\2011	cradmin (8man-demo\cradmin)	Vollzugriff	
13	\\srv-8man\Finanz\Assets\2011	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
14	\\srv-8man\Finanz\Assets\2012	cradmin (8man-demo\cradmin)	Vollzugriff	
15	\\srv-8man\Finanz\Assets\2012	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
16	\\srv-8man\Finanz\Gehälter	cradmin (8man-demo\cradmin)	Vollzugriff	
17	\\srv-8man\Finanz\Gehälter\Berlin	cradmin (8man-demo\cradmin)	Vollzugriff	
18	\\srv-8man\Finanz\Gehälter\München	cradmin (8man-demo\cradmin)	Vollzugriff	
19	\\srv-8man\Finanz\nicht gucken	cradmin (8man-demo\cradmin)	Vollzugriff	
20	\\srv-8man\Finanz\nicht gucken	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
21	\\srv-8man\Finanz\nicht gucken\steuerdaten	cradmin (8man-demo\cradmin)	Vollzugriff	
22	\\srv-8man\Finanz\nicht gucken\steuerdaten	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
23	\\srv-8man\Finanz\nicht gucken\steuerdaten\Channel Islands	cradmin (8man-demo\cradmin)	Vollzugriff	
24	\\srv-8man\Finanz\nicht gucken\steuerdaten\Channel Islands	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
25	\\srv-8man\Finanz\nicht gucken\steuerdaten\schweiz	cradmin (8man-demo\cradmin)	Vollzugriff	
26	\\srv-8man\Finanz\nicht gucken\steuerdaten\schweiz	Arbeit, Andi (8man-demo\Andi Arbeit)	Lesen und Ausführen	
27	\\srv-8man\GF	cradmin (8man-demo\cradmin)	Vollzugriff	
28	\\srv-8man\GF\Audits	cradmin (8man-demo\cradmin)	Vollzugriff	
29	\\srv-8man\GF\DontTouch	cradmin (8man-demo\cradmin)	Vollzugriff	
30	\\srv-8man\GF\DontTouch\Secret	cradmin (8man-demo\cradmin)	Vollzugriff	
31	\\srv-8man\GF\Ganz wichtiger und geheimer Ordner	cradmin (8man-demo\cradmin)	Vollzugriff	
32	\\srv-8man\GF\Rezepte	cradmin (8man-demo\cradmin)	Vollzugriff	
33	\\srv-8man\GF\Rezepte\Toskana - Orange-Mango vollecker	cradmin (8man-demo\cradmin)	Vollzugriff	

Öffnen Sie den Report in Excel. 8MAN listet alle Verzeichnisse mit Direktberechtigungen auf.

5.3.2.6 Verzeichnisse identifizieren, deren Besitzer nicht Administratoren sind

Hintergrund / Mehrwert

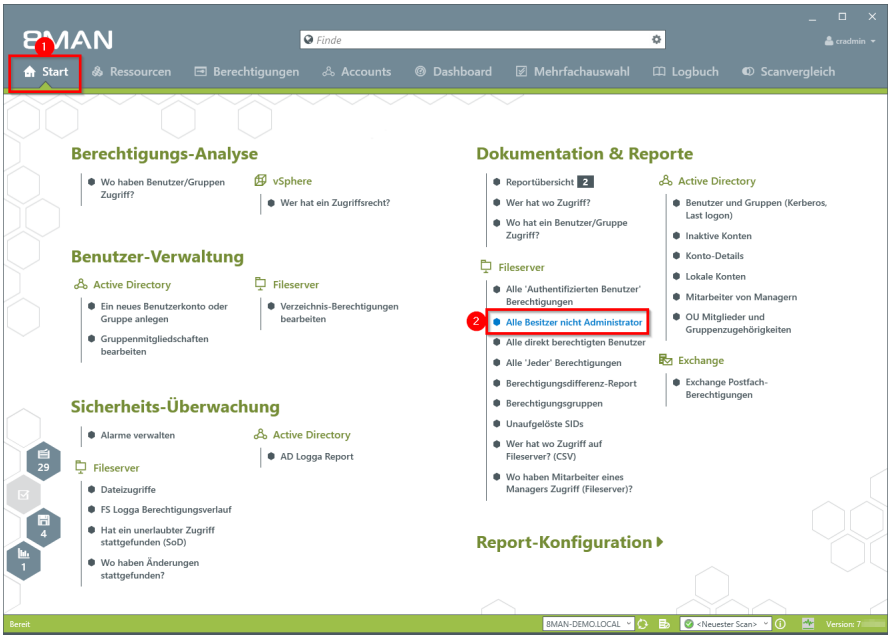
8MAN zeigt Ihnen auf Ihren Fileservern alle Verzeichnisse an, auf denen der Besitzer nicht die lokale Administratorengruppe ist.

Schließen Sie die User vom Besitz von Verzeichnissen aus, können Sie unerwünschte Berechtigungsänderungen verhindern.

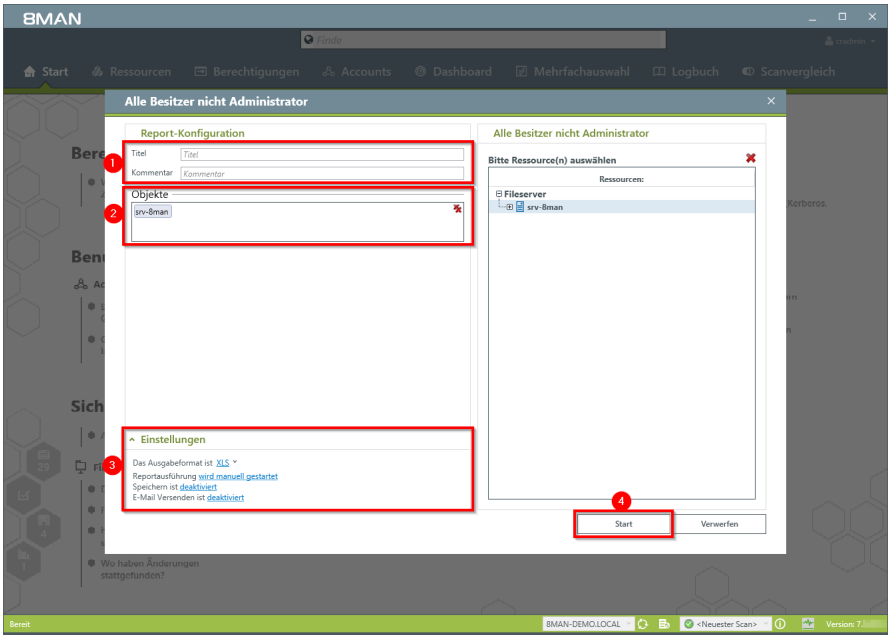
Weiterführende Services

Besitzer von Verzeichnissen ändern

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Alle Besitzer nicht Administrator".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.3.2.7 "Authentifizierte Benutzer" Berechtigungen identifizieren

Hintergrund / Mehrwert

Der Report zeigt alle Verzeichnisse, auf denen das Konto "Authentifizierte Benutzer" berechtigt ist. Dieses technische Nutzerkonto sollte wie das "Jeder Konten" niemals auf nicht öffentliche Ressourcen berechtigt sein.

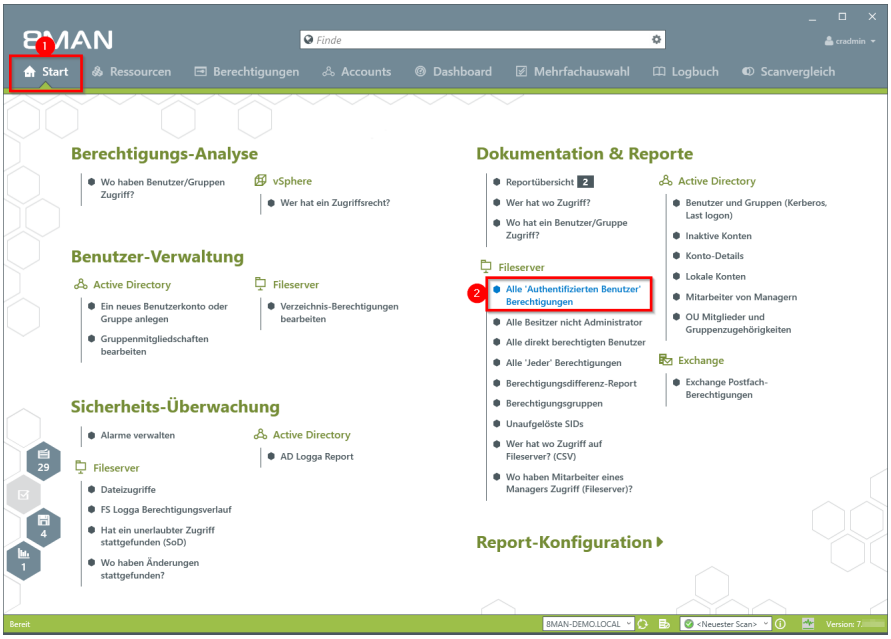
Prüfen Sie den Report auf sicherheitsrelevante Verzeichnisse und entfernen Sie die Berechtigung für "Authentifizierte Benutzer".

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 4.247 Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista.

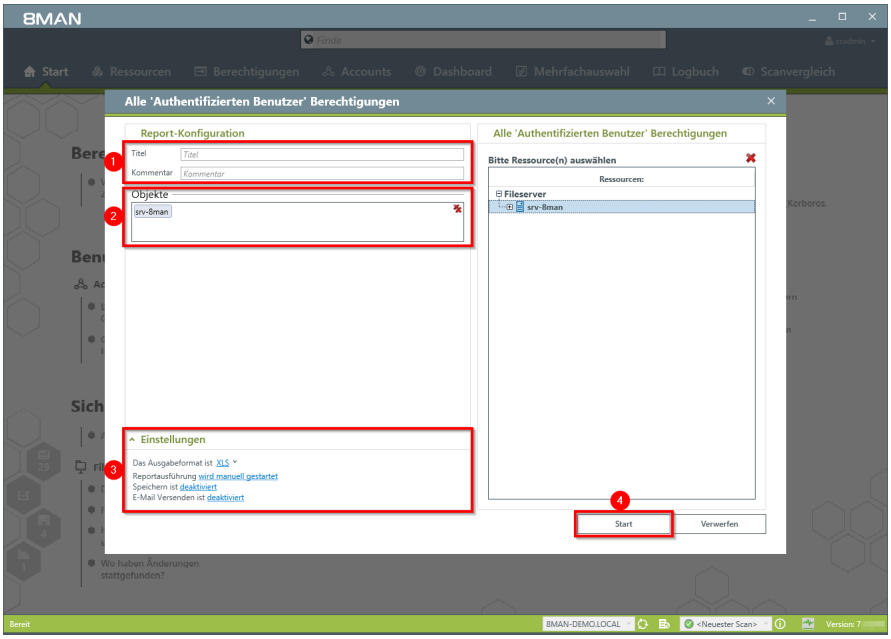
Weiterführende Services

"Jeder" Berechtigungen identifizieren
Global zugängliche Verzeichnisse identifizieren (Webclient)
"Jeder" Berechtigungen im bulk entfernen (Webclient)

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Alle Besitzer nicht Administrator".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.4 +8MATE for Exchange

Im Bereich Documentation & Reporting bietet das Addon 8MATE for Exchange folgende Services:

Report: Wer hat wo Zugriff?
Report: Postfach Berechtigungen identifizieren

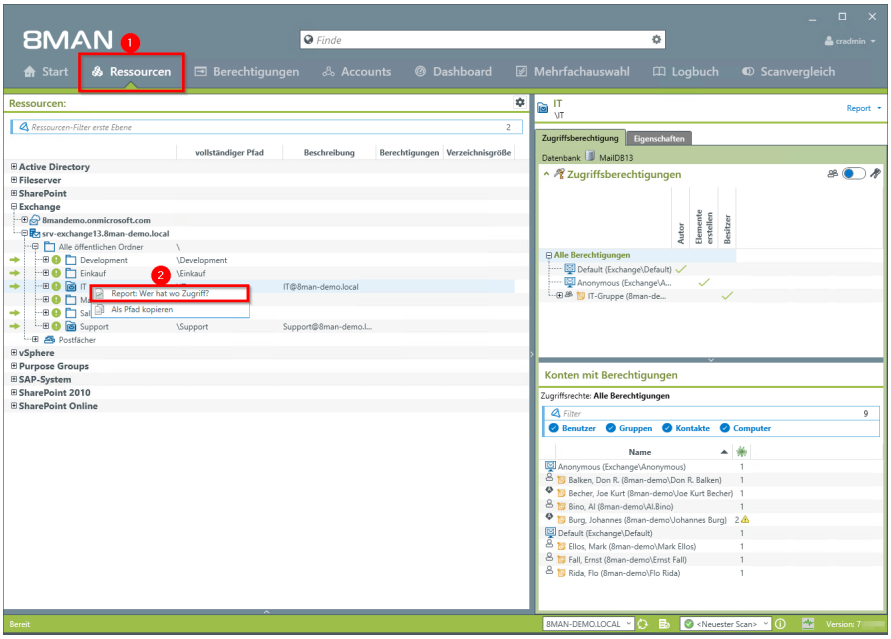
5.4.1 Reporte für Führungskräfte

5.4.1.1 Wer hat wo Zugriff?

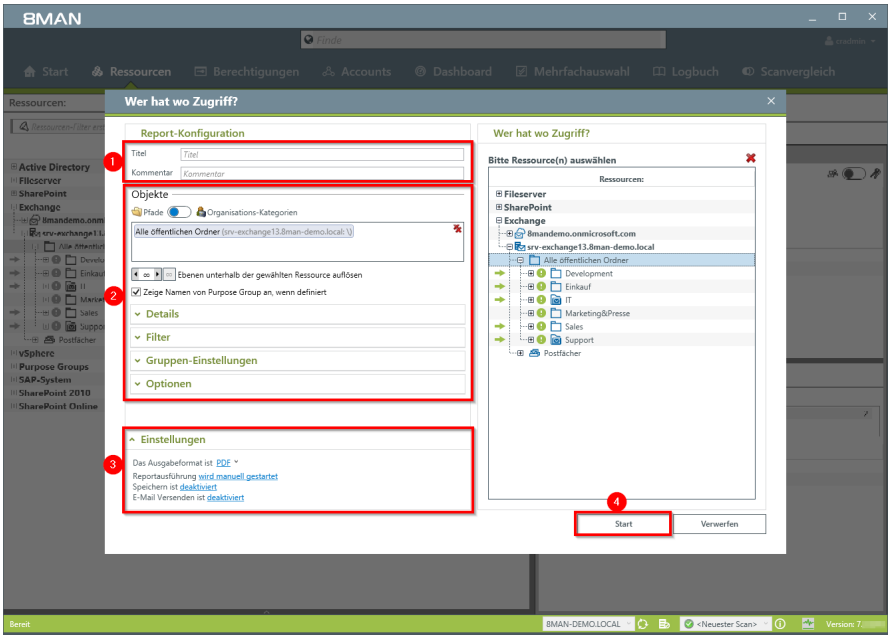
Hintergrund / Mehrwert

Führungskräfte wissen am besten, wer worauf Zugriff haben sollte. Insbesondere für öffentliche Exchange Ordner und Postfächer muss vollständig Transparenz bestehen. Der Report "Wer hat wo Zugriff?" bietet eine Übersicht über alle Personen und deren Rechte auf öffentliche Ordner. Darüber hinaus wird das sicherheitskritische Recht "Senden als" auf Postfächern angezeigt.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Rechtsklicken Sie einen oder alle öffentlichen Ordner. Wählen Sie im Kontextmenü "Report: Wer hat wo Zugriff?".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports. Zur Komplexitätsreduktion empfehlen wir im Bereich "Gruppen-Einstellungen" im Auswahlmenü "Benutzeransicht" zu wählen.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.4.1.2 Postfach Berechtigungen identifizieren

Hintergrund / Mehrwert

8MAN erzeugt Reporte, in denen die Postfach-Berechtigungen angezeigt werden. Dazu zählen:

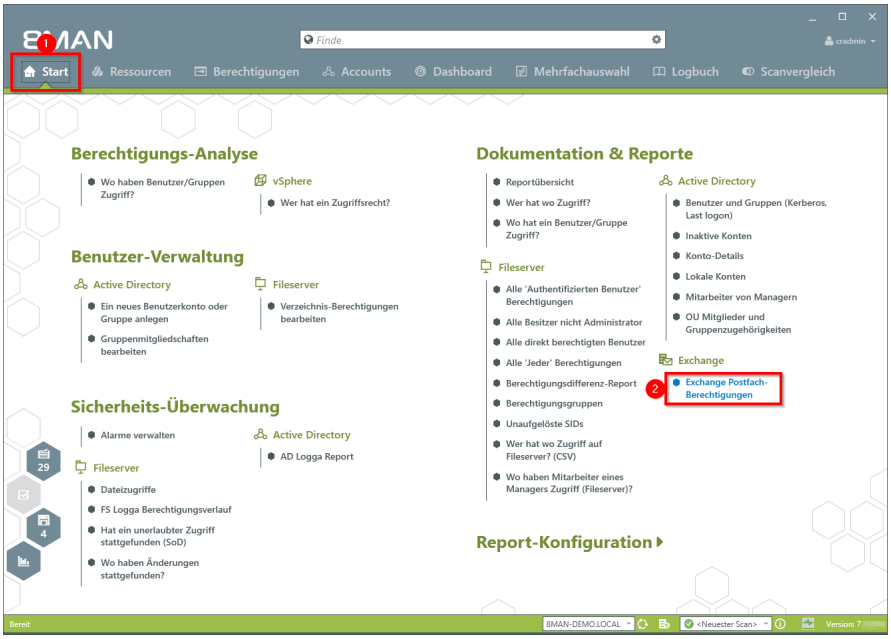
- Postfachverzeichnisse mit ihren Berechtigungen
- Eigenschaften (Postfachgrößen)
- Stellvertreter für Postfächer
- Abwesenheitsnotizen

Sicherheitsrelevant sind insbesondere die Postfachverzeichnisse mit ihren Berechtigungen. Bei diesen finden sich in der Praxis häufig Überberechtigungen. Da in den Ordnern sensible E-Mails liegen können, muss hier ein Transparenz geschaffen werden.

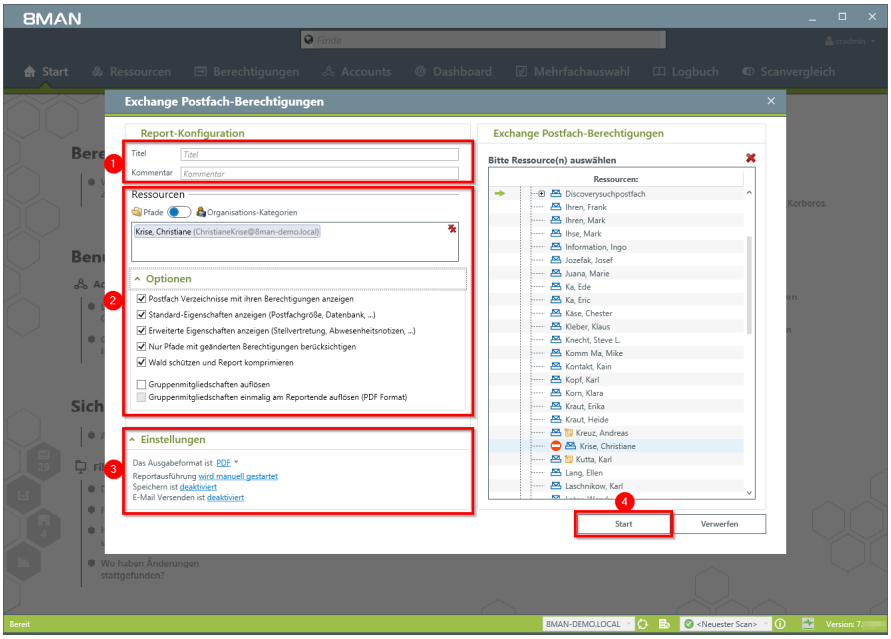
Weiterführende Services

Die sicherheitskritischen "Senden als" - Berechtigungen werden im Report "Wer hat wo Zugriff?" dargestellt.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Exchange Postfach-Berechtigungen".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.5 +8MATE for Sharepoint

Im Bereich Documentation & Reporting bietet das Addon 8MATE for Sharepoint folgende Services:

Report: Wer hat wo Zugriff?
Report: Wo haben Benutzer/Gruppen Zugriff?

5.5.1 Reporte für Führungskräfte

5.5.1.1 Wer hat wo Zugriff?

Hintergrund / Mehrwert

Führungskräfte wissen am besten wer worauf Zugriff haben sollte. Insbesondere für sensible SharePoint Sites muss vollständig Transparenz bestehen. Der Report "Wer hat wo Zugriff?" bietet eine Übersicht über alle Rechte und Personen, die diese Rechte auf der Site ausüben können.

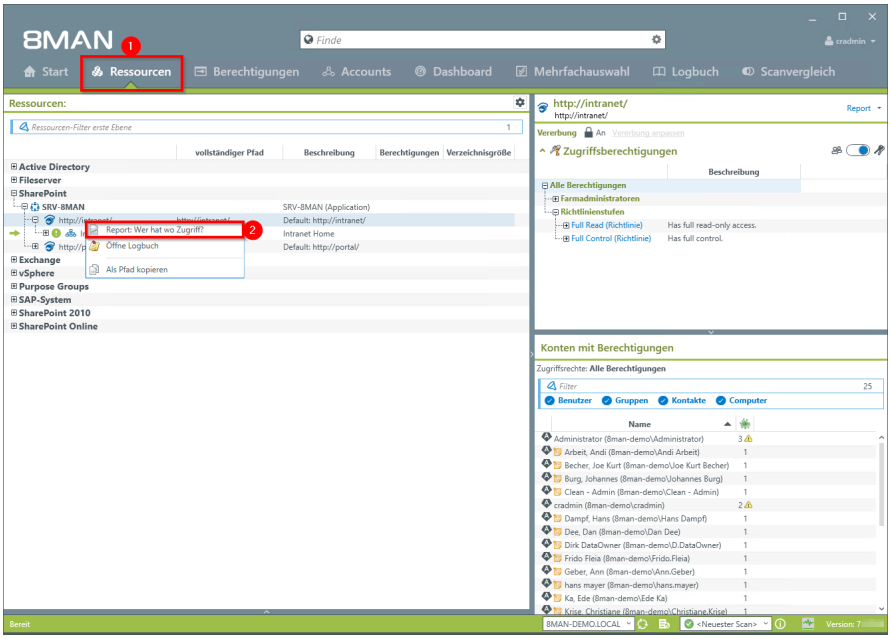
Der Report gibt der verantwortlichen Führungskraft eine Entscheidungsgrundlage, um zwei zentrale Fragen zu beantworten:

- Wer sollte Zugriff haben? (Erhöhung der Datensicherheit)
- Welche Zugriffsrechte sollten bestehen? (Erhöhung von Datenintegrität)

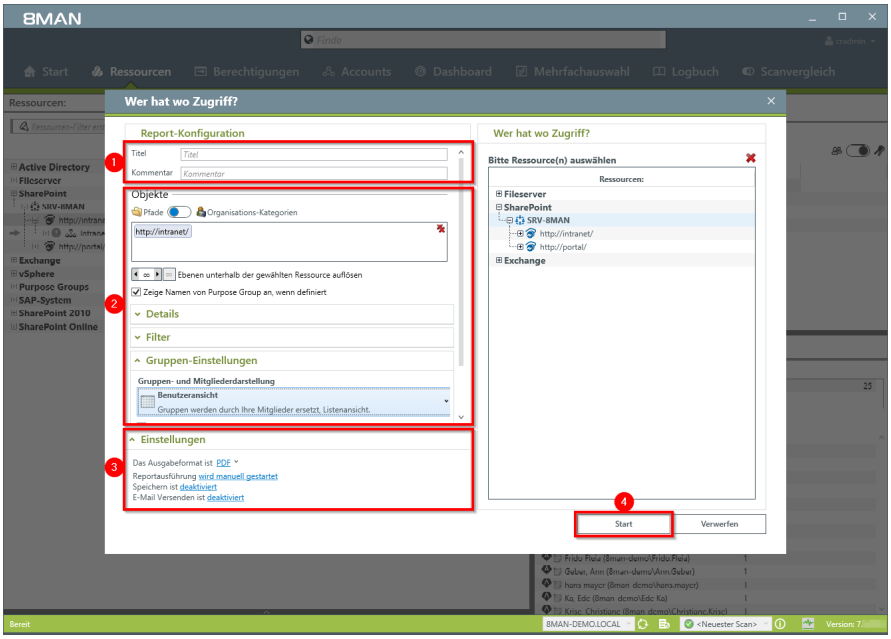
Weiterführende Services

Berechtigungen auf SharePoint Ressourcen ändern

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Rechtsklicken Sie eine SharePoint Ressource. Wählen Sie im Kontextmenü "Report: Wer hat wo Zugriff?".*



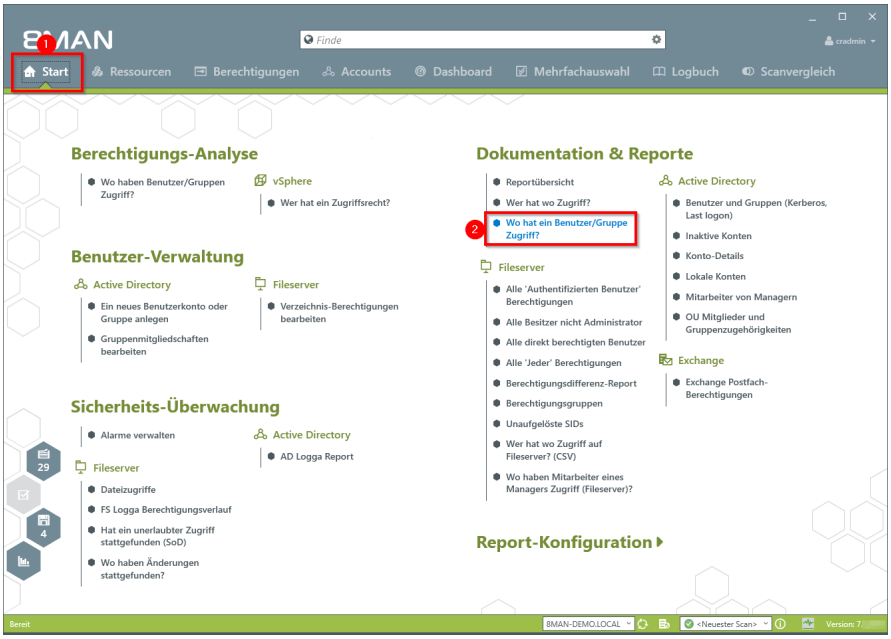
1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports. Zur Komplexitätsreduktion empfehlen wir im Bereich "Gruppen-Einstellungen" im Auswahlmenü "Benutzeransicht" zu wählen. Die restlichen Einstellungen richten sich an Experten.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

5.5.1.2 Wo haben Benutzer/Gruppen Zugriff?

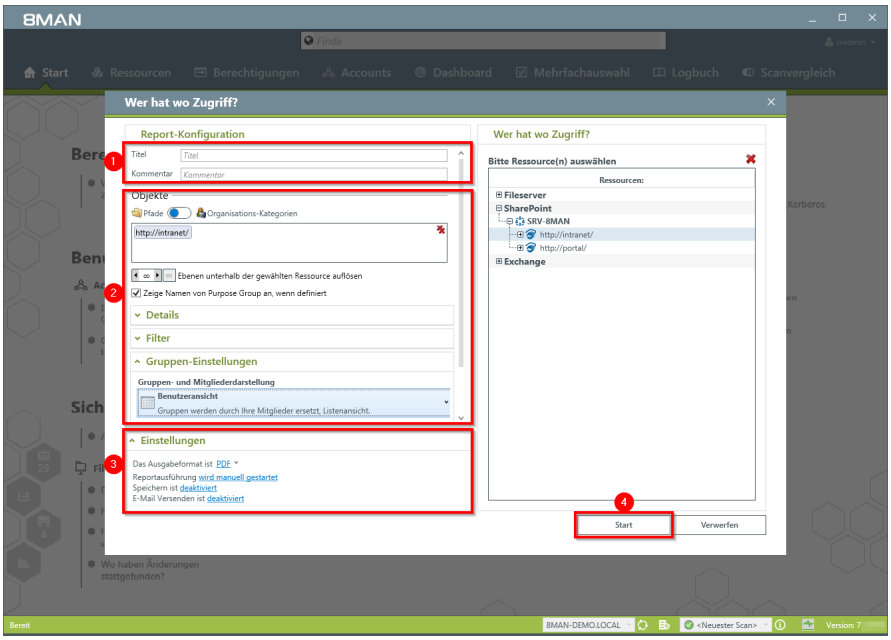
Hintergrund / Mehrwert

Der Report "Wo hat ein Benutzer/Gruppe Zugriff?" listet die Zugriffsrechte von Nutzerkonten und Gruppen auf ausgewählte Fileserver-Verzeichnissen in einem Dokument auf.

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Wo hat ein Benutzer/Gruppe Zugriff?".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports. Zur Komplexitätsreduktion empfehlen wir im Bereich "Gruppen-Einstellungen" im Auswahlmenü "Benutzeransicht" zu wählen. Die restlichen Einstellungen richten sich an Experten.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

6. Security Monitoring

6.1 Active Directory

6.1.1 +8MATE AD Logga

Problem

Auf dem AD führen eine Reihe von Mitarbeitern Änderungen aus. Ohne ein vollumfängliches Monitoring entstehen Sicherheitsrisiken und Unstimmigkeiten in den Prozessen.

Sicherheitsrisiken

Sicherheitsrisiken entstehen, wenn temporäre Gruppenmitgliedschaften unautorisierten Mitarbeitern Zugriff auf vertrauliche Dokumente geben. Werden die Gruppenmitgliedschaften anschließend wieder entzogen, bleibt der Sicherheitsvorfall unerkannt.

Unklare Prozesse

Unklare Prozesse können nur verbessert werden, wenn die Ist-Prozesse analysierbar sind. Wer gibt wem Mitgliedschaften und setzt Passwörter zurück? Wo entstehen Probleme und sind Absprachen nötig? Durch die Analyse von Fehlern, lässt sich ein individuelles Gruppenvergabekonzept erstellen.

Lösung

Der 8MAN schafft Klarheit über die Berechtigungssituation im Active Directory. Der AD Logga erweitert diese Transparenz auf die gesamte Änderungshistorie im System. Dabei werden auch außerhalb vom 8MAN vorgenommene Aktivitäten erfasst. Sicherheitsrelevante temporäre Gruppenmitgliedschaften und daraus resultierende unkontrollierte Berechtigungsvergaben sind damit sofort nachvollziehbar.

Anhand konfigurierbarer Reporte lassen sich Aktivitäten im Hinblick auf Konten, Objekten, Gruppen und Attribute lückenlos aufdecken.

Das erreichen Sie mit dem AD Logga

- Administratoren erhalten ein vollständiges Bild über die Aktivitäten im AD. Prozesse können so optimiert werden.
- Auditoren erkennen Sicherheitsvorfälle und die involvierten Akteure. Maßnahmen können so ergriffen werden.
- Die Geschäftsführung hat die Gewissheit: Der AD Logga stellt mit seinem Monitoring die Daten für interne Sicherheit und Prozessverbesserungen bereit.
- Die AD Logga Alarme informieren sie proaktiv. Sollte jemand sicherheitsrelevante Konten oder Gruppen manipulieren, wird der Administrator sofort informiert.

6.1.1.1 Änderungen im Active Directory überwachen (Report)

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga überwachen Sie die Ist-Prozesse in ihrem Active Directory. Das Besondere: Auch mit Bordmitteln durchgeführte, temporäre Änderungen werden erfasst. Aus sicherheitskritischer Sicht sind insbesondere Veränderungen an Ereignistypen und Ereignisautoren wichtig:

Überwachung von Ereignistypen

Änderungen an:

- Attributen
- Benutzern
- Computern
- Gruppen
- Kennwörtern
- Konten
- Mitgliedern

Überwachung von Ereignisautoren

- Benutzer
- Gruppen
- Computer

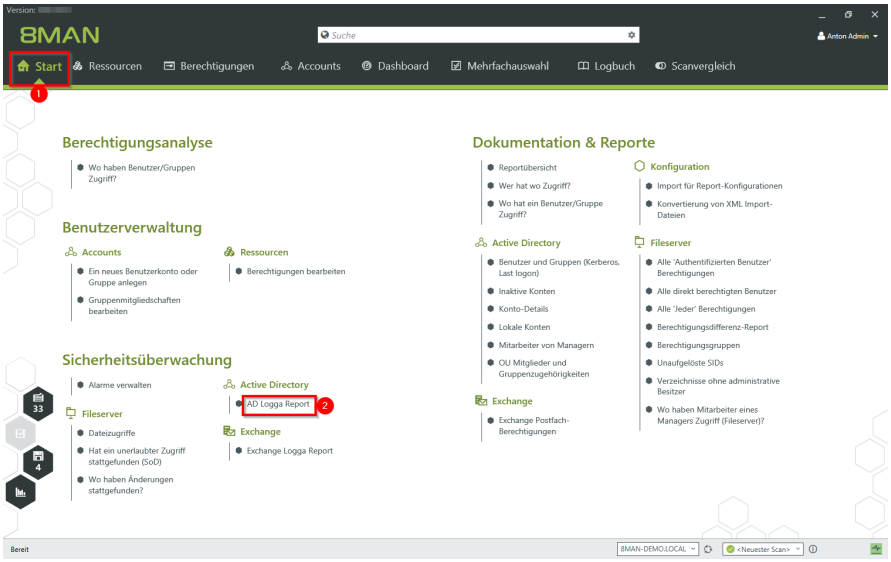
Zusätzlich können Sie noch nach Objekt Klassen und Attributen filtern. Dabei handelt es sich jedoch um Experteneinstellungen. Filtern Sie nach einem seltenen Attribut, kann dies die gesamte Suche verfremden.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle sowie M 4.312 Überwachung von Verzeichnisdiensten.

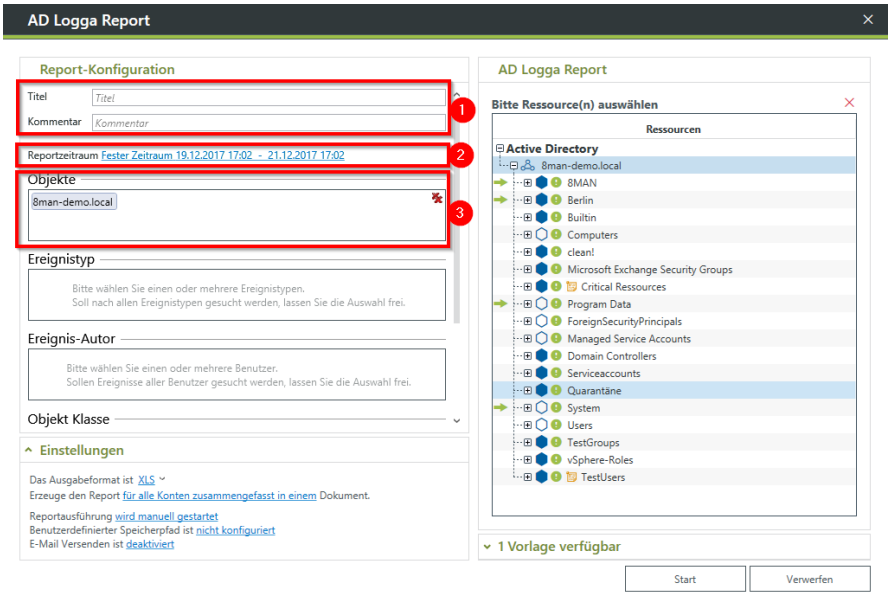
Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten
Alarme für Gruppen anlegen
Alarme für Nutzerkonten anlegen

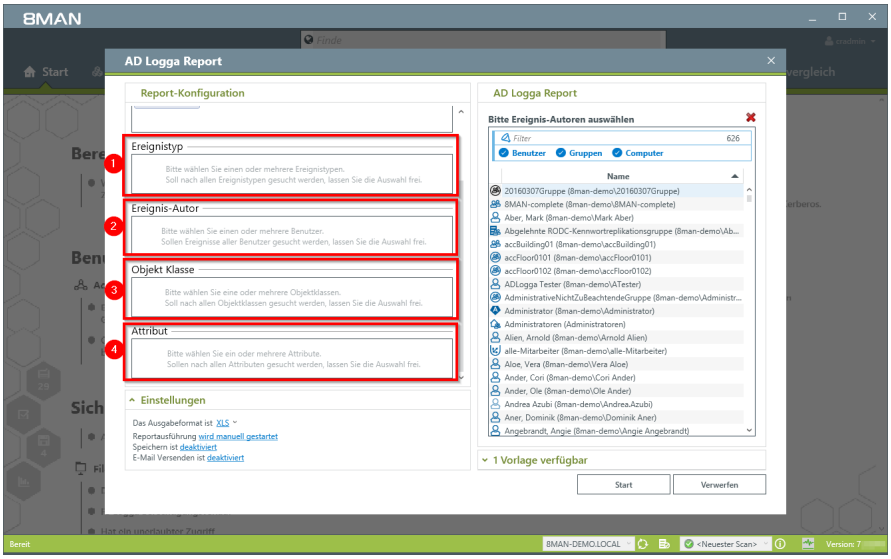
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "AD Logga Report".*

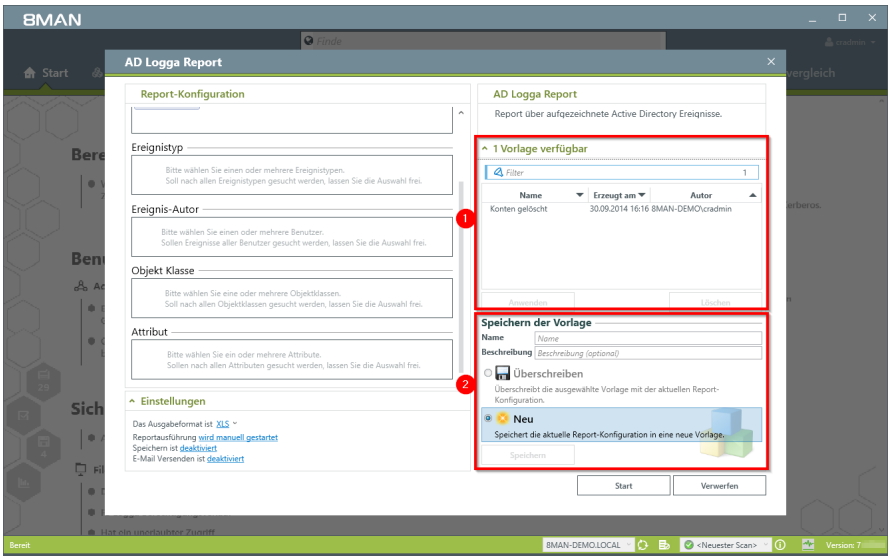


1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Legen Sie den Zeitraum für den Report fest.*
3. *Wählen Sie die Domänenobjekte, deren Ereignisse im Report enthalten sein sollen.*



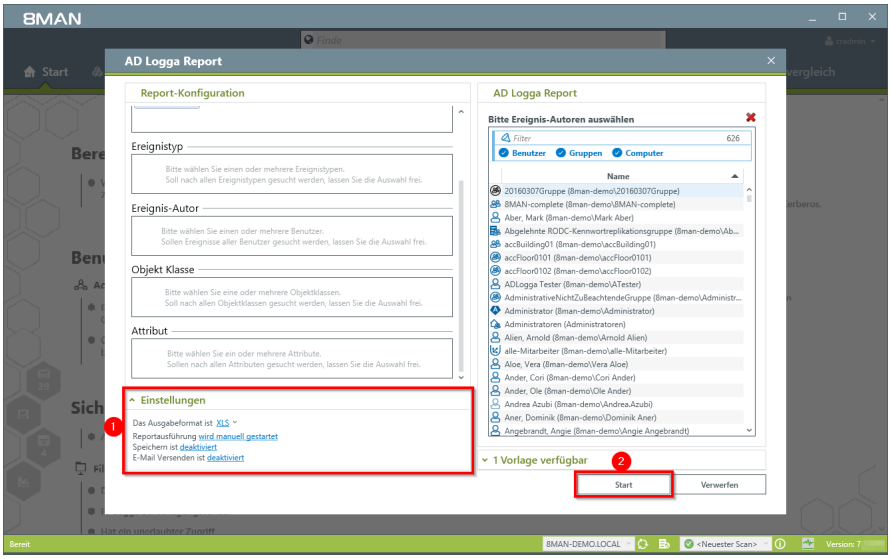
Definieren Sie den Umfang des Reports, in dem Sie die folgenden Filter setzen. Für alle Filter gilt: Sollen alle aufgezeichneten Ereignisse im Report enthalten sein, lassen Sie die Auswahl frei.

1. *Fügen Sie die Typen von Ereignissen hinzu.*
2. *Fügen Sie die Autoren von Ereignissen hinzu.*
3. *Fügen Sie die Objektklassen hinzu.*
4. *Fügen Sie die Attribute von Ereignissen hinzu.*



Sie können AD Logga Reportkonfigurationen als Vorlagen speichern. Erleichtern Sie sich so die Wiederverwendung von komplexen Reportkonfigurationen.

1. *Wählen Sie eine vorhandene Vorlage.*
2. *Speichern Sie die aktuelle Konfiguration als Vorlage.*



1. *Legen Sie verschiedene Ausgabeoptionen fest.*
2. *Starten Sie die Erstellung des Reports.*

6.1.1.2 Temporäre Gruppenmitgliedschaften erkennen

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga schliessen Sie eine zentrale Sicherheitslücke: Temporäre Gruppenmitgliedschaften.

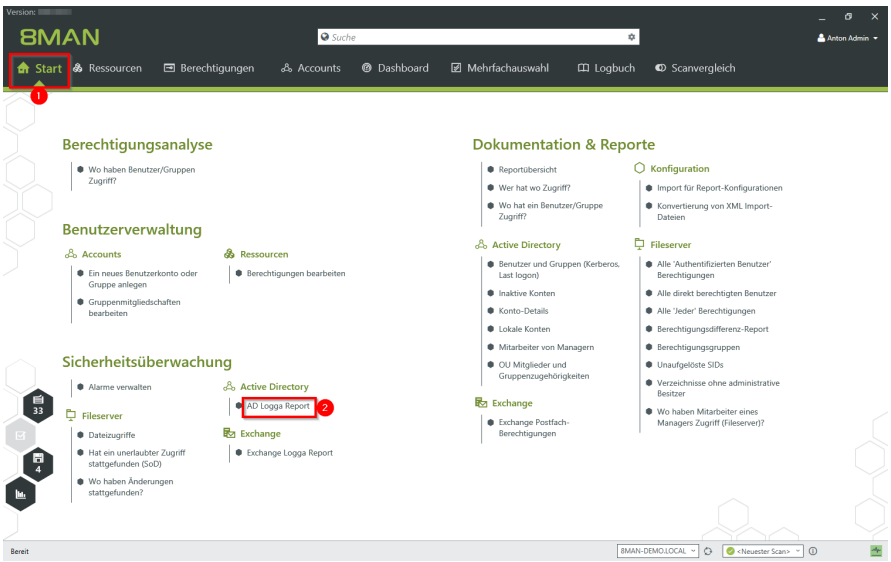
Innentäter berechtigen sich auf geheime Verzeichnisse, kopieren Daten und stellen den Ursprungszustand der Berechtigungssituation wieder her. Ohne AD Logga bleiben Aktionen wie diese unter dem Radar.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 4.312 Überwachung von Verzeichnisdiensten.

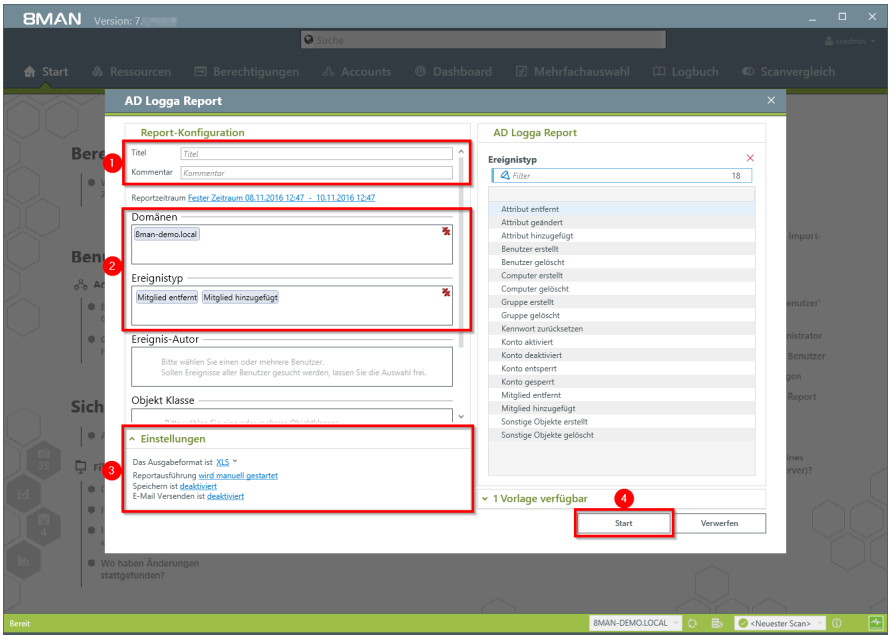
Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten
Alarme für Gruppen anlegen
Alarme für Nutzerkonten anlegen

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "AD Logga Report".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Legen Sie den Umfang des Reports fest. Wählen Sie bei Ereignistyp "Mitglied entfernt" und "Mitglied hinzugefügt".*
3. *Legen Sie Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

6.1.1.3 Gesperrte Benutzerkonten identifizieren

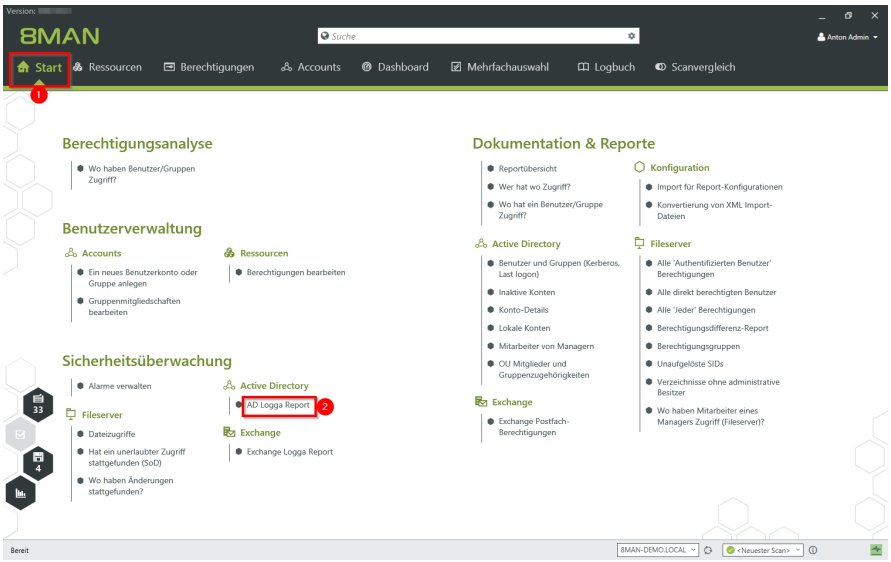
Hintergrund / Mehrwert

Der versuchte Login mit einem fremden Konto endet im besten Fall mit einem gesperrten Nutzerkonto. Der AD Logga zeigt Ihnen, von welchem Computer der Angriff kam.

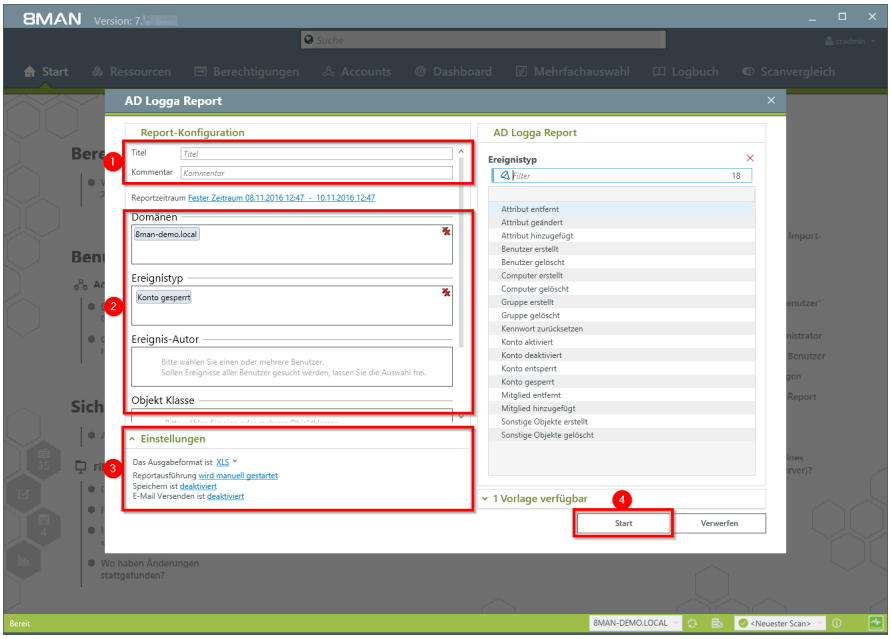
Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten
Alarme für Gruppen anlegen
Alarme für Nutzerkonten anlegen

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "AD Logga Report".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Legen Sie den Umfang des Reports fest. Wählen Sie bei Ereignistyp "Konto gesperrt".*
3. *Legen Sie Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

6.1.1.4 Kennwortzurücksetzungen überwachen

Hintergrund / Mehrwert

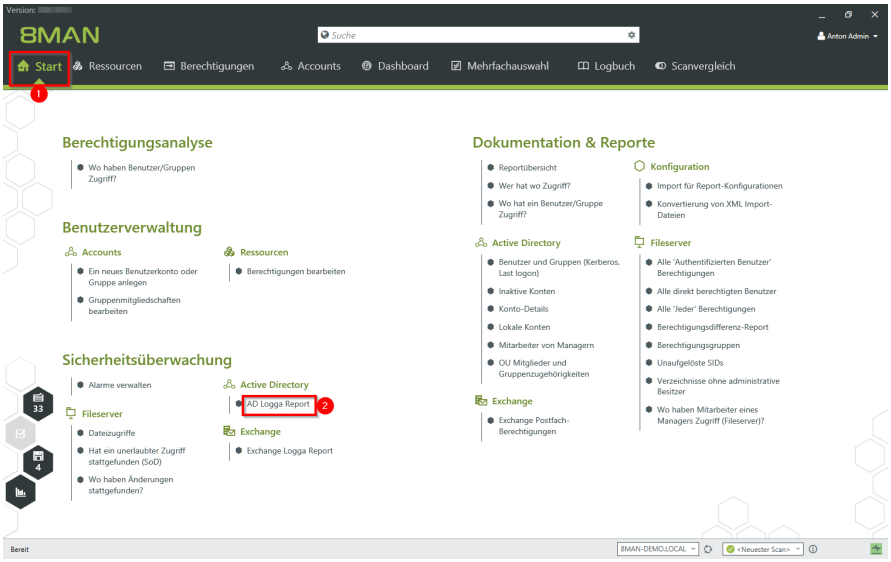
Mit dem 8MATE AD Logga überwachen Sie den Prozess des Kennwortrücksetzens. Diesem ist ein Sicherheitsrisiko inhärent. Setzt beispielsweise ein Helpdesk-Mitarbeiter heimlich das Kennwort einer Führungskraft zurück, kann er mit dem Übergangspasswort sich anmelden und geheime Daten einsehen. Die betroffene Führungskraft würde den Vorfall wahrscheinlich nicht merken und sich nur über das nicht mehr gültige Kennwort wundern, den Support kontaktieren und ein neues Kennwort erhalten.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.11 Regelung des Passwortgebrauchs, M 4.48 Passwortschutz unter Windows-Systemen sowie M 4.312 Überwachung von Verzeichnisdiensten.

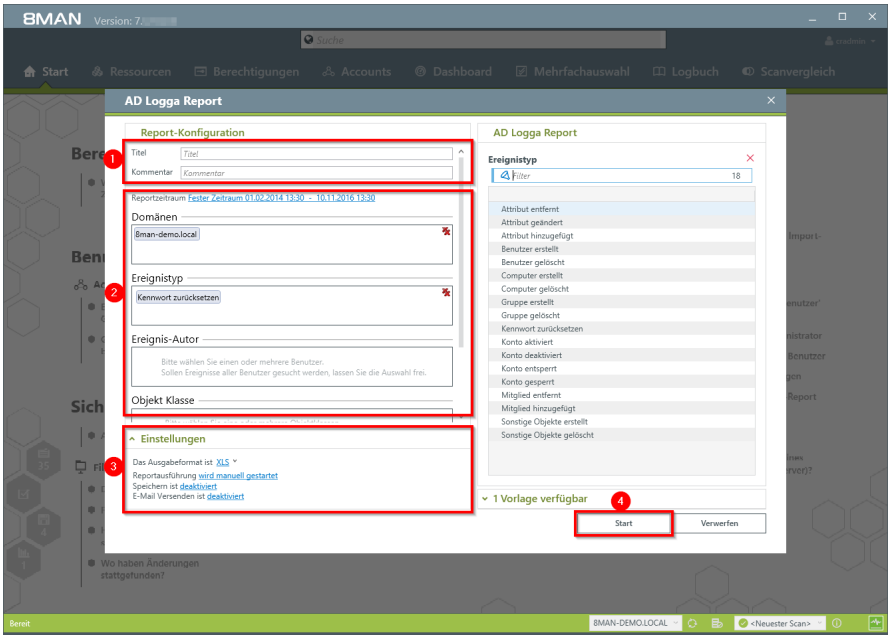
Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten
Alarme für Gruppen anlegen
Alarme für Nutzerkonten anlegen

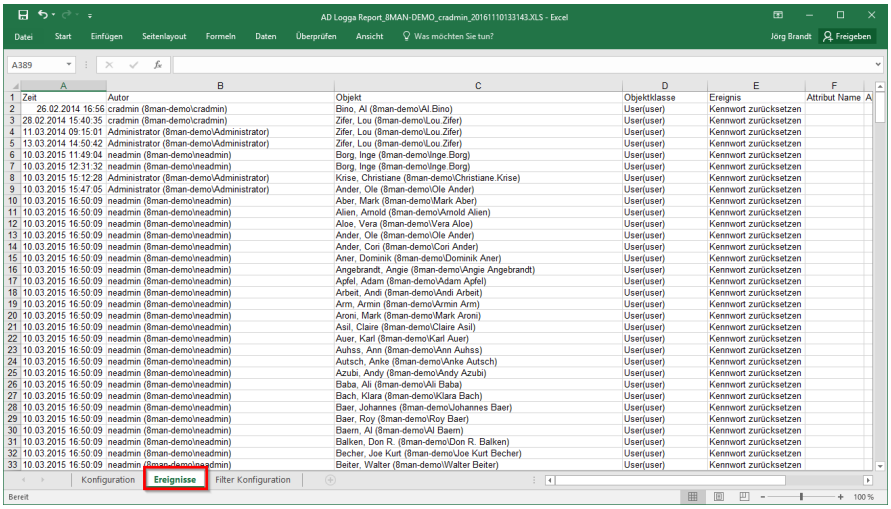
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "AD Logga Report".*



1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Legen Sie den Umfang des Reports fest. Wählen Sie bei Ereignistyp "Kennwort zurücksetzen".*
3. *Legen Sie Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*



Öffnen Sie den Report in Excel. Auf dem Tabellenblatt "Ereignisse" listet der Report die Passwort-Rücksetzungen auf.

6.1.1.5 AD Logga Ereignisse mit dem Logbuch auswerten

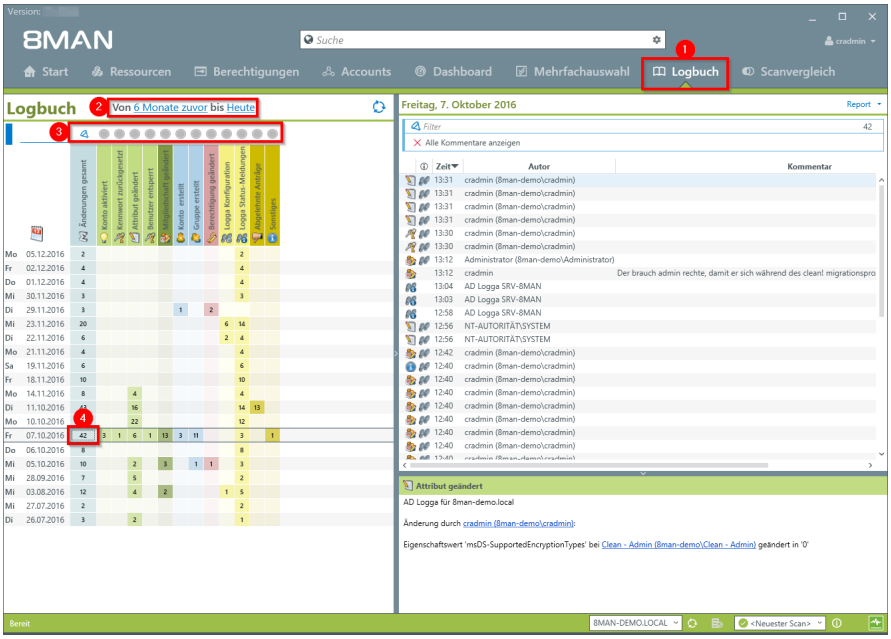
Hintergrund / Mehrwert

Mit dem 8MATE AD Logga aufgezeichnete Ereignisse können Sie mit den Reportfunktionen detailliert und wiederkehrend analysieren. Schneller beantworten Sie konkrete Fragen zu AD-Änderungen mit der Logbuchansicht.

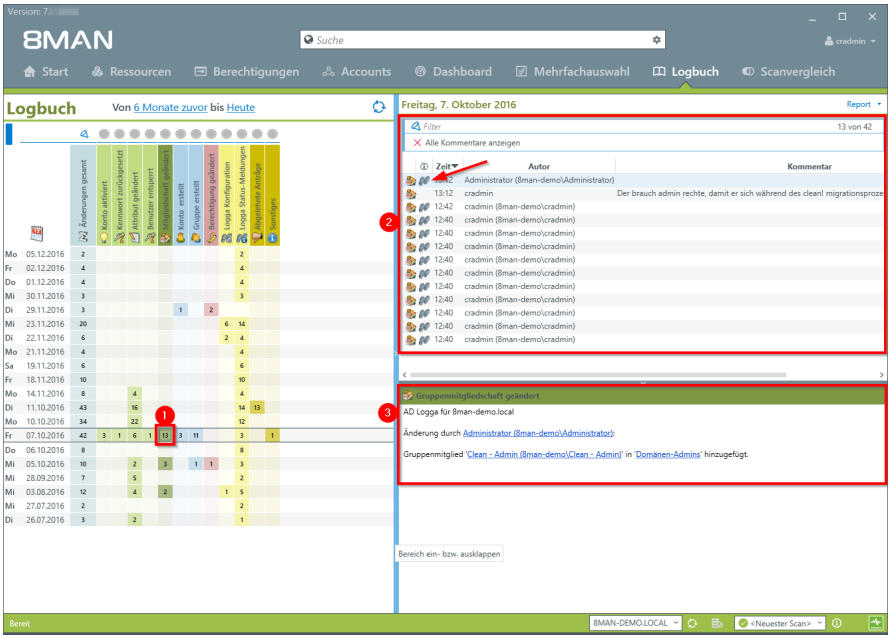
Weiterführende Services

Änderungen im Active Directory überwachen
Temporäre Gruppenmitgliedschaften erkennen
Gesperrte Benutzerkonten identifizieren
Kennwortrücksetzungen überwachen
Alarme für Gruppen anlegen
Alarme für Nutzerkonten anlegen

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Logbuch".*
2. *Legen Sie den Zeitraum für die Logbuch-Analyse fest.*
3. *Über die Filter fokussieren Sie auf die Events, die Sie prüfen möchten.*
4. *Selektieren Sie alle Ereignisse eines Tages (eine Zeile).*



1. *Selektieren Sie eine Zelle (einen Ereignistyp), um Ihre Abfrage weiter einzugrenzen.*
2. *8MAN zeigt eine Liste aller gewählten Ereignisse. An dem "Fußspuren-Symbol" erkennen Sie vom AD Logga aufgezeichnete Ereignisse. Selektieren Sie ein Ereignis.*
3. *8MAN zeigt alle Details zum Ereignis.*

6.1.1.6 Alarme für Gruppen anlegen

Hintergrund / Mehrwert

Über Gruppenmitgliedschaften erhalten Mitarbeiter ihre Zugriffsrechte im Firmennetzwerk. Besonders schützenswerte Gruppen verleihen ihren Mitgliedern Rechte auf geheime Ordner und wichtige Ressourcen. Mit dem im 8MATE AD Logga können Sie AD Gruppen aktiv überwachen und sollten neue Mitglieder hinzugefügt werden, einen Alarm auslösen.

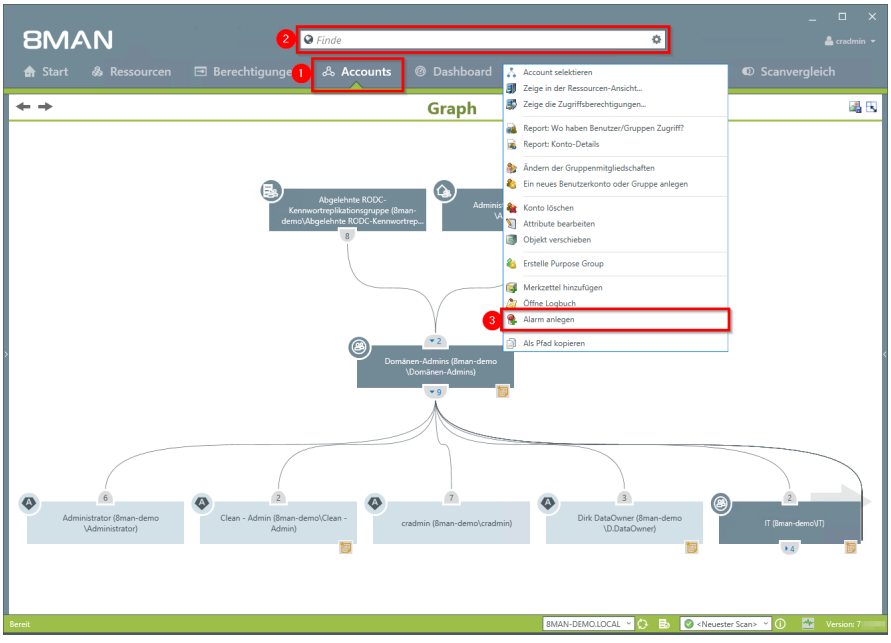
Die Gruppenverschachtelungen im Active Directory machen es notwendig, auch Gruppenmitgliedschaften zu überwachen, die sich aus neuen, indirekten Mitgliedschaften ergeben. Ein Beispiel: Die Gruppe „Geschäftsführer“ wird überwacht und hat als Mitglied die Gruppe „geheime Daten“. 8MATE AD Logga Alarme benachrichtigen Sie jetzt auch, wenn der letztgenannten Gruppe neue Mitglieder oder Gruppen hinzugefügt bzw. entfernt werden.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle sowie M 4.312 Überwachung von Verzeichnisdiensten.

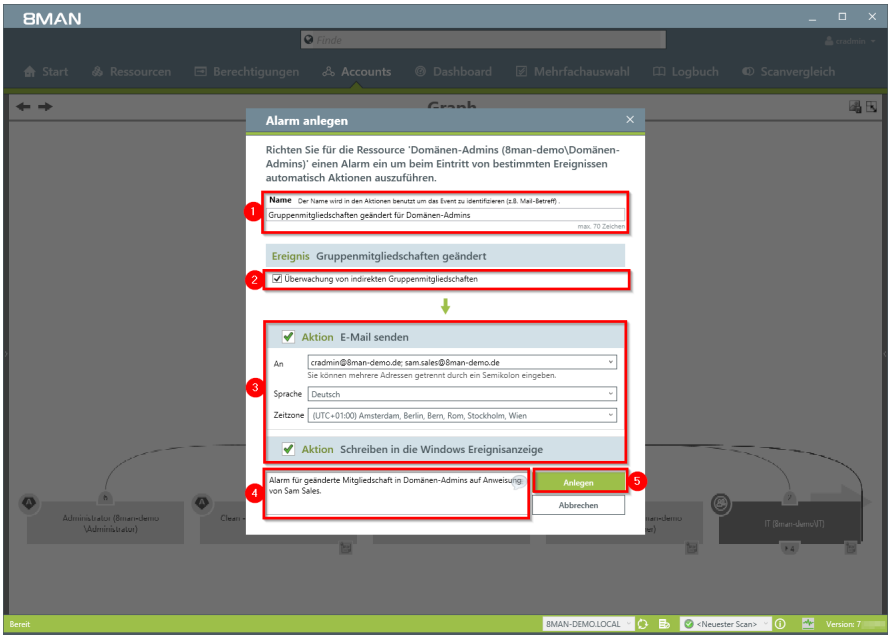
Weiterführende Services

Alarmsensoren aktivieren/deaktivieren
Alarme für Nutzerkonten anlegen
Alarme verwalten

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Accounts".*
2. *Finden Sie die gewünschte Gruppe mit der Suchfunktion.*
3. *Rechtsklicken Sie die Gruppe und wählen "Alarm anlegen" im Kontextmenü.*



1. *Geben Sie dem Alarm einen Namen.*
2. *Aktivieren Sie die Checkbox, um auch über indirekte Änderungen an den Gruppenmitgliedschaften informiert zu werden.*
3. *Sie können beliebig viele E-Mail-Empfänger hinterlegen. Darüber hinaus kann der Alarm auch in die Windows Ereignisanzeige geschrieben werden.*
4. *Sie müssen einen Kommentar hinterlegen.*
5. *Aktivieren Sie den Alarm.*

6.1.1.7 Alarme für Nutzerkonten anlegen

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga überwachen Sie den Prozess des Kennwortrücksetzens. Diesem ist ein Sicherheitsrisiko inhärent. Setzt beispielsweise ein Helpdesk-Mitarbeiter heimlich das Passwort einer Führungskraft zurück, kann er mit dem Übergangspasswort sich anmelden und geheime Daten einsehen. In diesem Fall sind bei aktivierter Alerts Funktion die kontrollierenden Instanzen informiert.

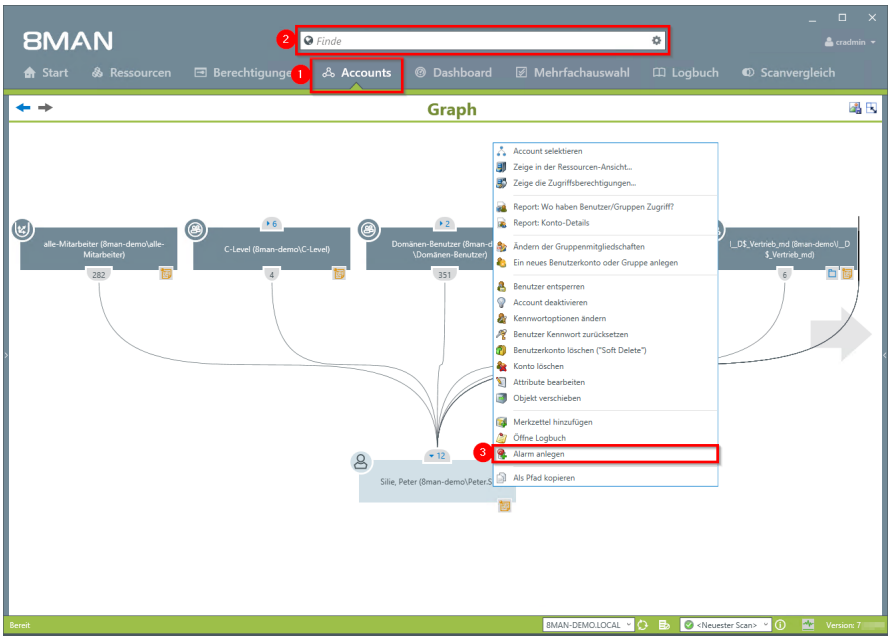
Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle sowie M 4.312 Überwachung von Verzeichnisdiensten.

Weiterführende Services

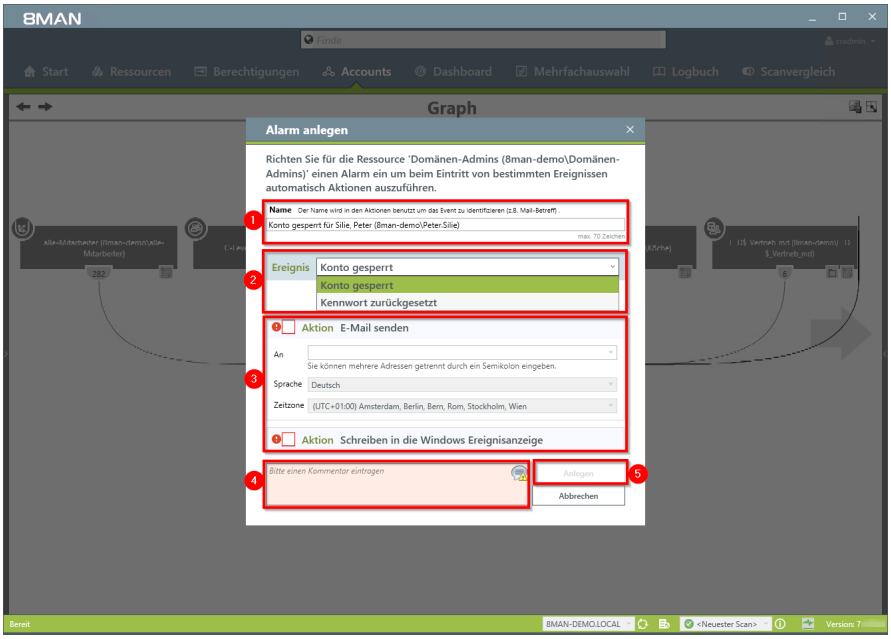
Alarmsensoren aktivieren/deaktivieren

Alarme für Gruppen anlegen

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Accounts".*
2. *Finden Sie den gewünschten Benutzer mit der Suchfunktion.*
3. *Rechtsklicken Sie den Benutzer und wählen "Alarm anlegen" im Kontextmenü.*



1. *Geben Sie dem Alarm einen Namen.*
2. *Wählen Sie ein Ereignis, über das Sie informiert werden.*
3. *Sie können beliebig viele E-Mail-Empfänger hinterlegen. Darüber hinaus kann der Alarm auch in die Windows Ereignisanzeige geschrieben werden.*
4. *Sie müssen einen Kommentar hinterlegen.*
5. *Aktivieren Sie den Alarm.*

6.1.1.8 Nach einem Alarm ein Skript ausführen

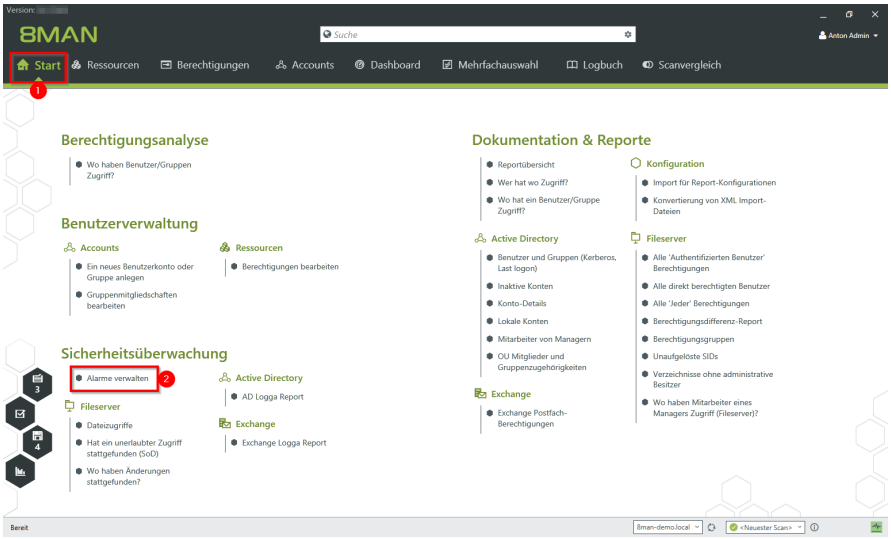
Hintergrund / Mehrwert

Starten Sie ein Skript, nachdem der FS Logga oder der AD Logga einen Alarm ausgelöst haben. Zum Beispiel überwachen Sie eine sicherheitskritische Gruppe auf Mitgliedschaftsänderungen und setzen, nachdem der Alarm ausgelöst wurde, automatisch die Mitgliedschaft wieder auf den Standard zurück.

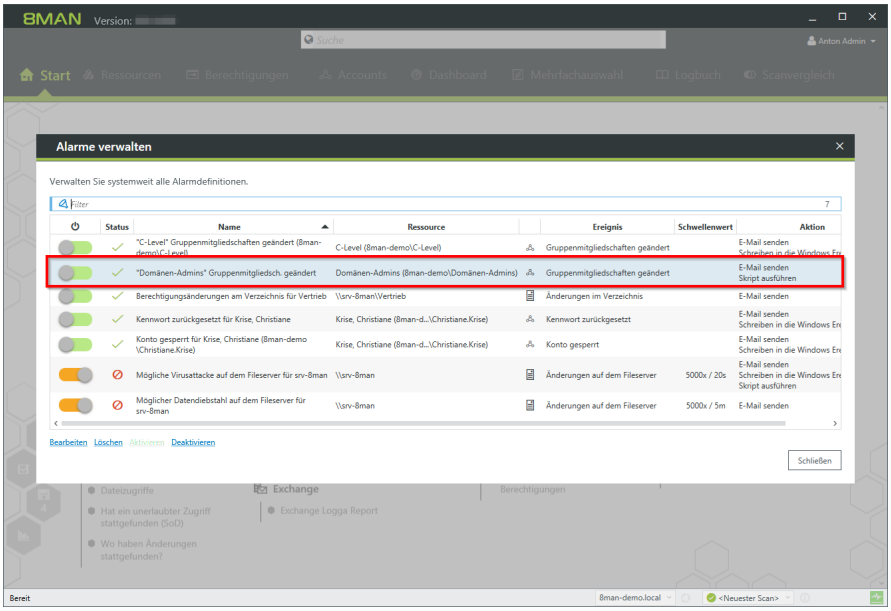
Weiterführende Services

Alarme verwalten

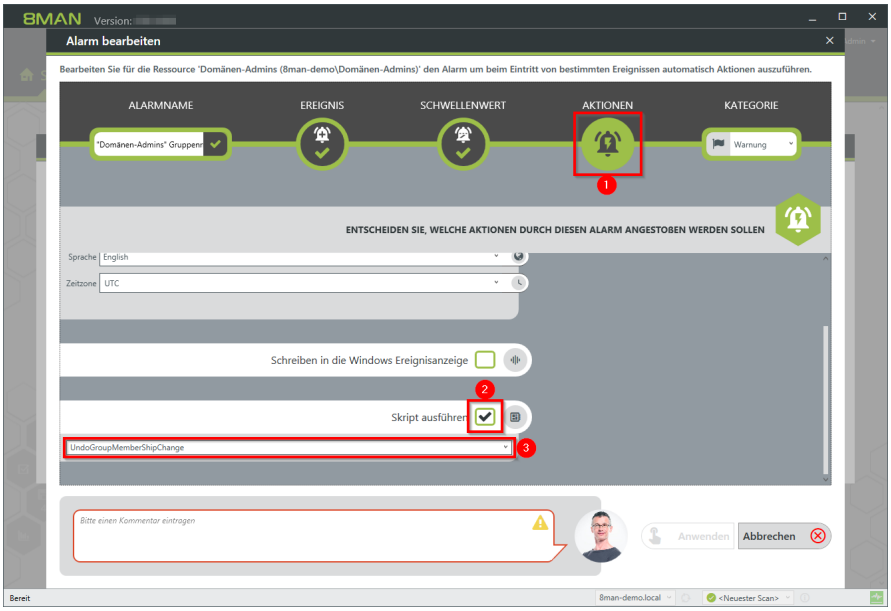
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Alarme verwalten".*



Doppelklicken Sie einen Eintrag.



1. *Wählen Sie "Aktionen".*
2. *Aktivieren Sie die Skriptausführung.*
3. *Wählen Sie ein Skript aus.*

Um die Option aktivieren zu können, muss eine Skriptkonfiguration für Alarme hinterlegt sein.

6.1.1.9 Alarme verwalten

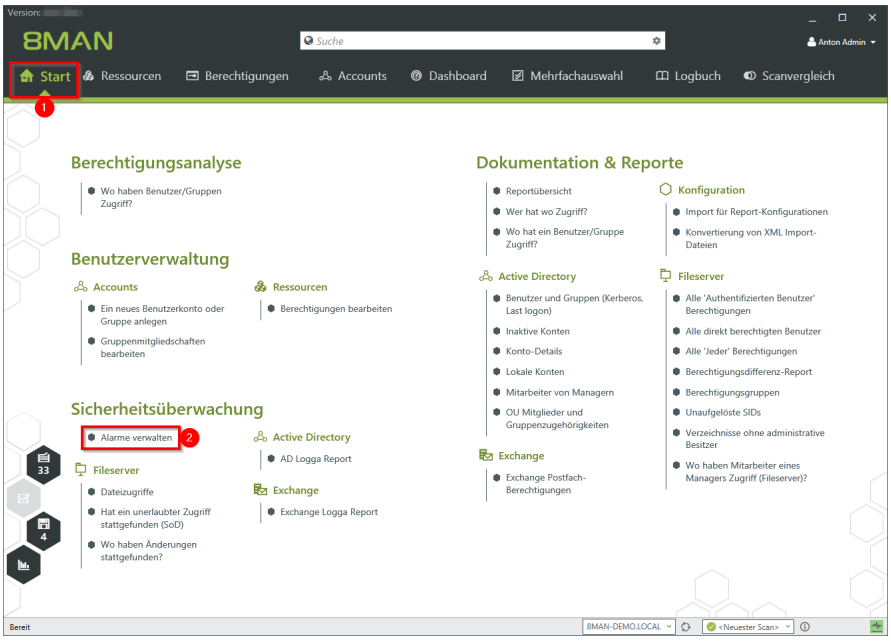
Hintergrund / Mehrwert

Sie können gesetzte Alarme jederzeit anpassen. Die Verwaltung erfolgt auf der 8MAN Startseite.

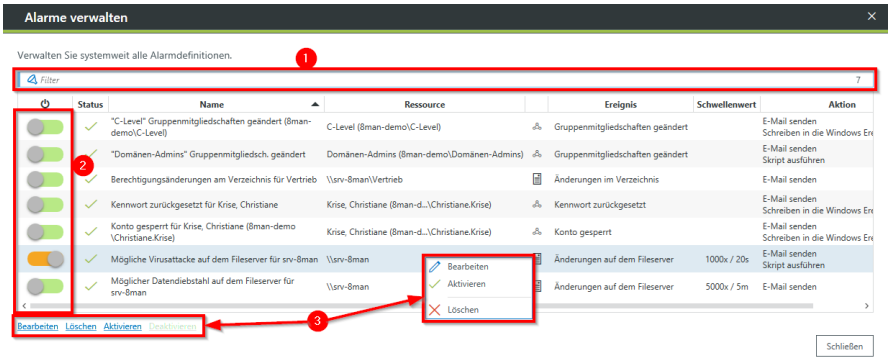
Weiterführende Services

Alarmsensoren aktivieren/deaktivieren

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Wählen Sie "Alarme verwalten".*



8MAN zeigt Ihnen alle Alarmkonfigurationen.

1. *Suchen Sie nach einer Alarmkonfiguration.*
2. *Schalten Sie Alarme ein oder aus.*
3. *Mit Rechtsklick oder den Links löschen, bearbeiten oder aktivieren/deaktivieren Sie die selektierte Alarmkonfiguration.*

6.2 Fileserver

6.2.1 +8MATE FS Logga

Sicherheitsrisiken

Sicherheitsrisiken entstehen, wenn temporäre Berechtigungen unautorisierten Mitarbeitern Zugriff auf vertrauliche Dokumente geben. Diese können eingesehen, gelöscht oder kopiert werden.

Werden die Rechte anschließend wieder entzogen, bleibt der Sicherheitsvorfall unerkannt. Wer was kopiert hat, lässt sich nicht mehr nachvollziehen.

Unklare Prozesse

Unklare Berechtigungsvergaben können nicht verbessert werden, wenn die Ist-Prozesse nicht analysierbar sind. Wer gibt wem Rechte und warum?

Wo entstehen Probleme und wo sind Absprachen nötig? Durch die Analyse von Fehlern lässt sich ein individuelles Berechtigungskonzept erstellen.

Lösung

Der 8MAN schafft Klarheit über die Berechtigungssituation auf dem Fileserver. Der FS Logga erweitert diese Transparenz auf die gesamte Zugriffs- und Änderungshistorie im System. Dabei werden auch außerhalb vom 8MAN vorgenommene Aktivitäten erfasst. Sicherheitsrelevante temporäre Berechtigungen und Veränderungen an überwachten Verzeichnissen sind sofort nachvollziehbar.

Anhand konfigurierbarer Reporte lassen sich Berechtigungsänderungen aufdecken. Zugriffe und Veränderungen an sensiblen Dateien, wie löschen, kopieren, verschieben und schreiben, protokolliert der FS Logga lückenlos.

Das erreichen Sie mit dem FS Logga

- Administratoren erhalten ein vollständiges Bild über die Aktivitäten auf dem Fileserver. Berechtigungsprozesse können so optimiert werden.
- Auditoren erkennen Sicherheitsvorfälle bei sensiblen Dateien und können die involvierten Akteure ausmachen.
- Die Geschäftsführung hat die Gewissheit: Der FS Logga stellt mit seinem Monitoring die Daten für mehr Sicherheit und Prozessverbesserungen bereit und macht Missbrauch vollständig nachvollziehbar.

6.2.1.1 Die Zugriffe auf sensible Daten überwachen (Report)

Hintergrund / Mehrwert

Sie haben im ersten Schritt die Zugriffsrechte für sicherheitsrelevante Verzeichnisse eingeschränkt. Im zweiten Schritt empfehlen wir die permanente Überwachung der Zugriffe und von den Nutzern durchgeführte Aktionen. Dadurch erhalten Sie die vollständige Prozesstransparenz für besonders schützenswerte Daten und Informationen.

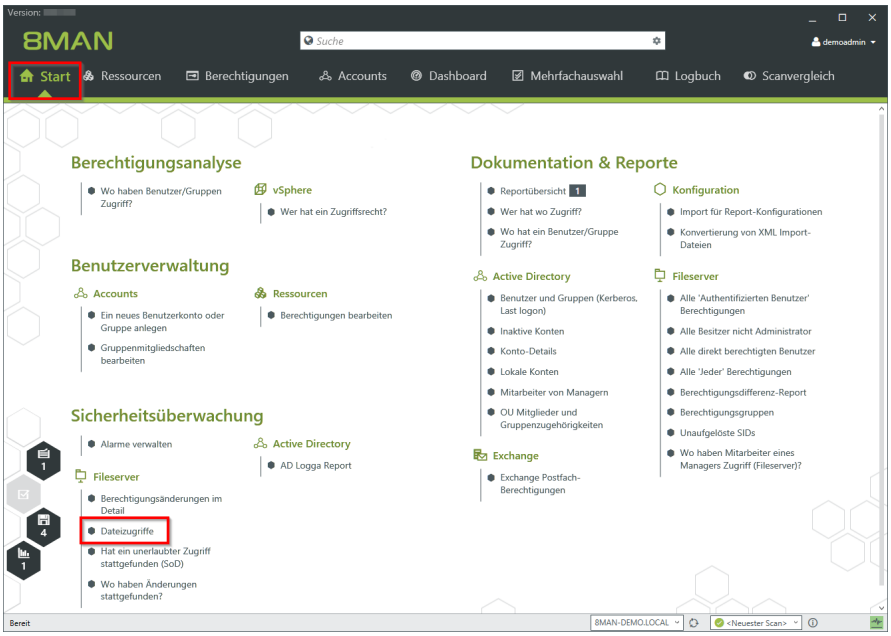
Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien.

Weiterführende Services

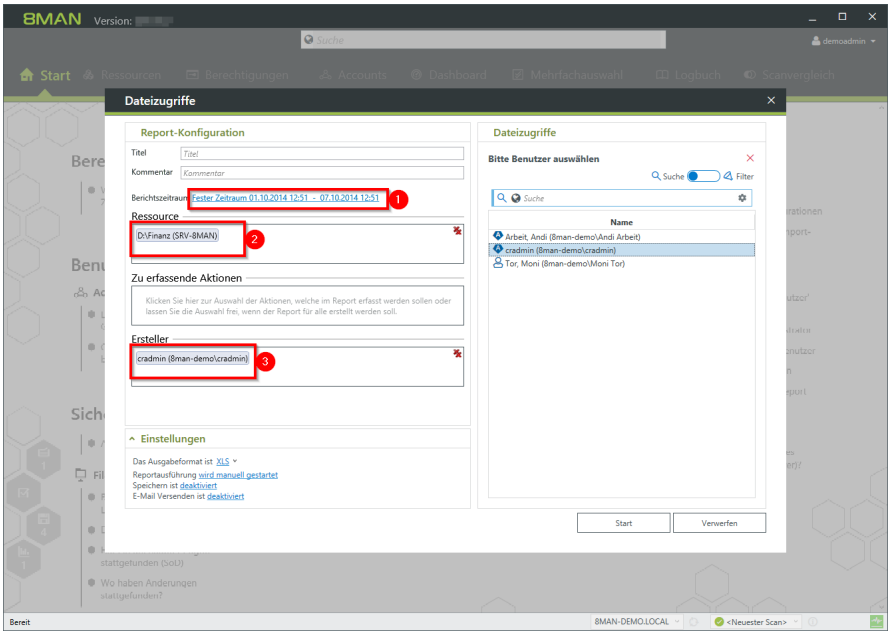
Prüfen und ändern Sie vorher die Verzeichnisberechtigungen, um die Akteure mit Zugriffsrechten einzuschränken:

Verzeichnisberechtigungen ändern

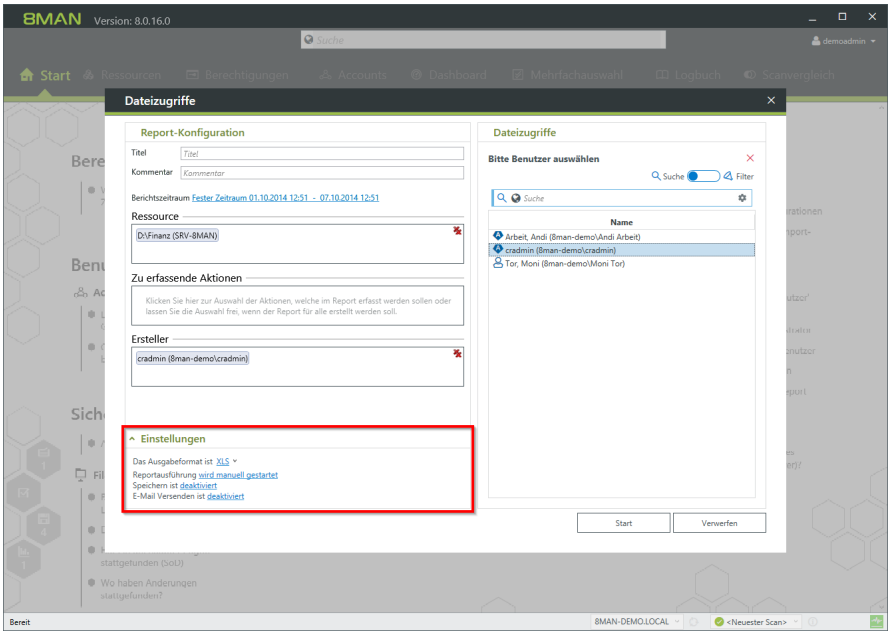
Der Prozess in einzelnen Schritten



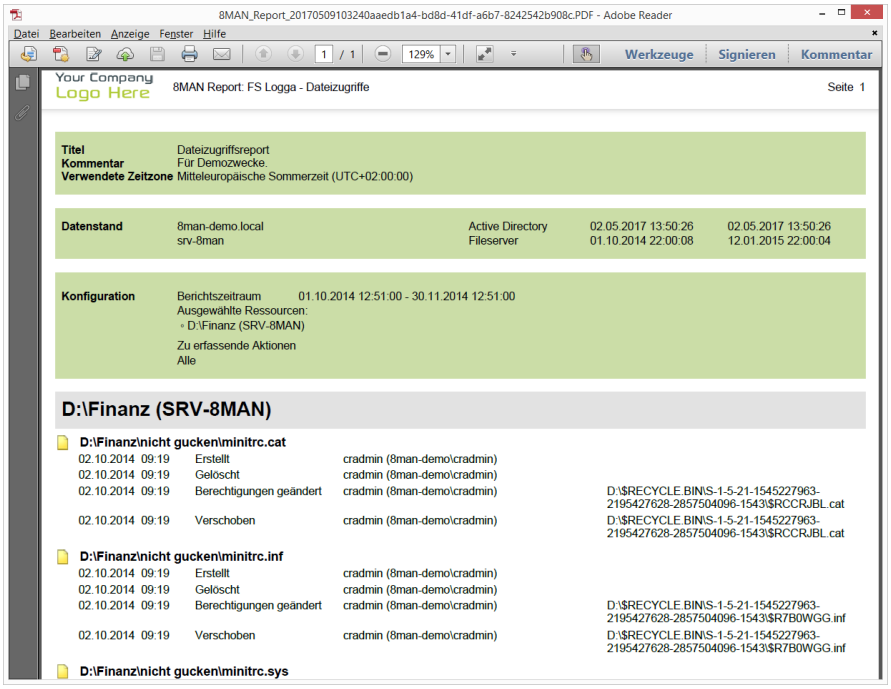
Wählen Sie auf der Startseite "Dateizugriffe".



1. *Legen Sie einen Zeitraum fest.*
2. *Optional: wählen Sie per Drag&Drop eine Ressource.*
3. *Optional: Wählen Sie einen Ersteller (Event-Autor)*



Planen Sie den FS Logga Report, versenden ihn per E-Mail oder speichern ihn auf dem Dateisystem.



Sie erhalten eine übersichtliche Auflistung über sämtlicher Dateiaktivitäten im gewählten Zeitfenster.

6.2.1.2 Alarme für Fileserververzeichnisse aktivieren

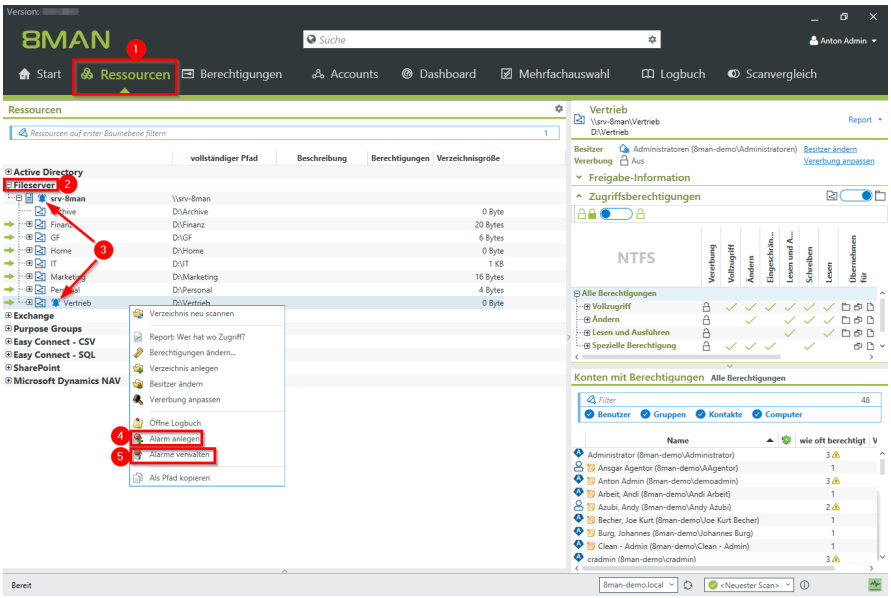
Hintergrund / Mehrwert

Überwachen Sie gezielt sicherheitskritische Verzeichnisse, indem Sie verzeichnisspezifische Alarme definieren. Sollte ein Zugriff auf ein sicherheitsrelevantes Verzeichnis erfolgen, sendet 8MAN einen Alarm an die Datenverantwortlichen.

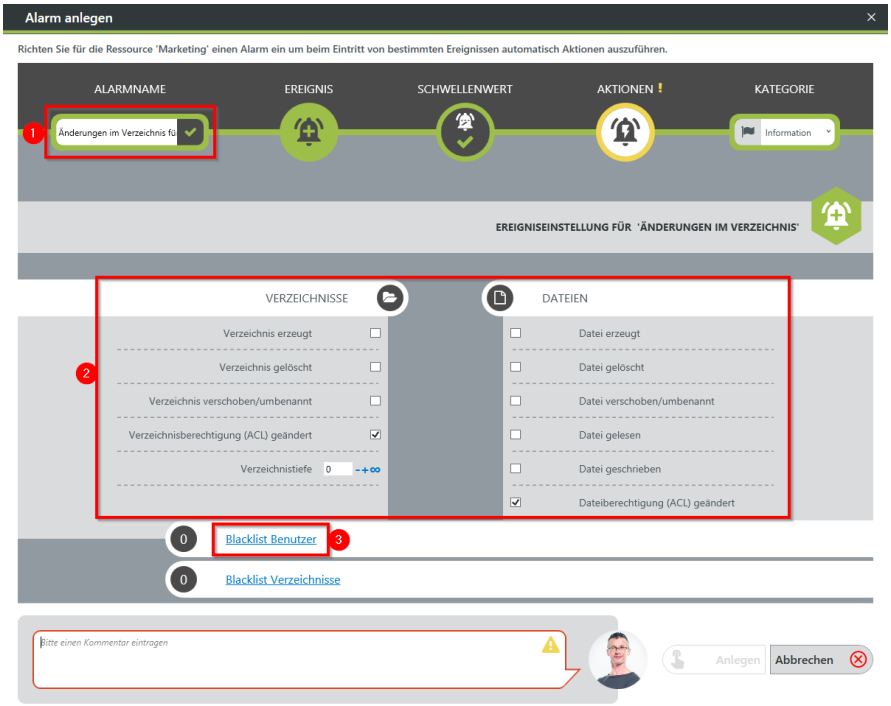
Weiterführende Services

Alarme für Verdachtsfälle auf Datendiebstahl aktivieren (Fileserver)
Alarme für Datenlöschungen aktivieren (Fileserver)
Alarme für Verdachtsfälle auf Ransomware aktivieren (Fileserver)
Nach einem Alarm ein Skript ausführen
Alarme verwalten

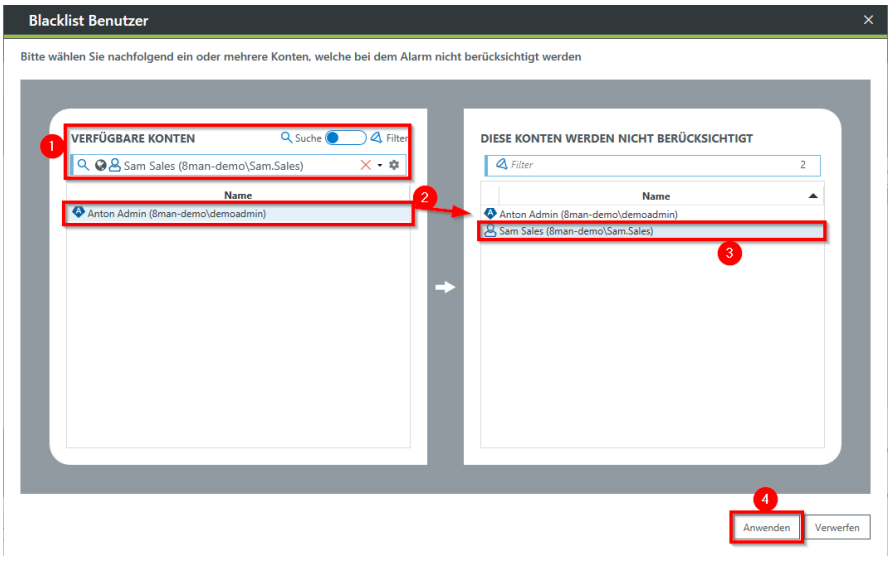
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Expandieren Sie den "Fileserver".*
3. *Bereits eingerichtete Alarme werden mit einem Glockensymbol dargestellt.*
4. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarm anlegen" im Kontextmenü, um einen neuen Alarm anzulegen.*
5. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarme verwalten" im Kontextmenü, um bestehende Alarme anzupassen oder zu löschen.*



1. *Geben Sie der Alarmkonfiguration einen Namen.*
2. *Legen Sie fest, welche Ereignisse einen Alarm auslösen.*
3. *Optional: Klicken Sie auf "Blacklist Benutzer".*



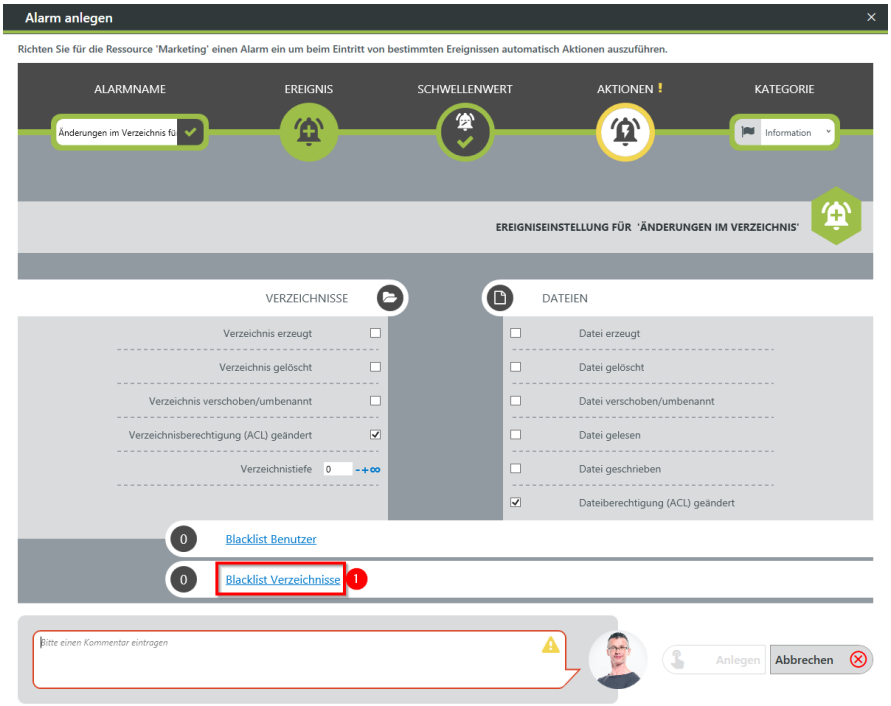
Optional:

Definieren Sie mit Hilfe der Blacklist, welche Benutzer keinen Alarm auslösen.

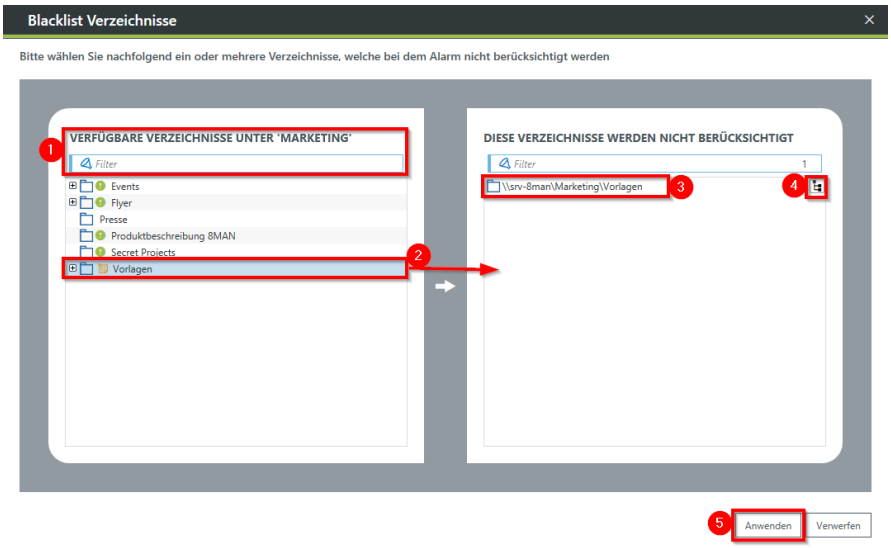
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

Sie können nur Benutzer hinzufügen, keine Gruppen.

1. *Nutzen Sie die Suchfunktion, um die gewünschten Benutzer zu finden.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Benutzer zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Benutzer von der Blacklist zu entfernen.*
4. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*



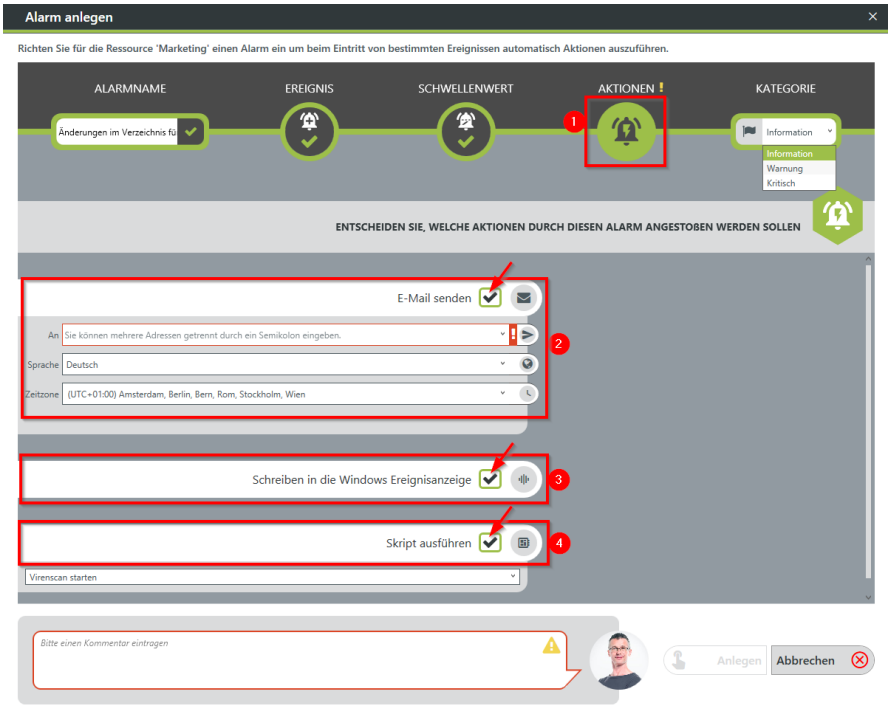
1. *Optional: Wählen Sie "Blacklist Verzeichnisse".*



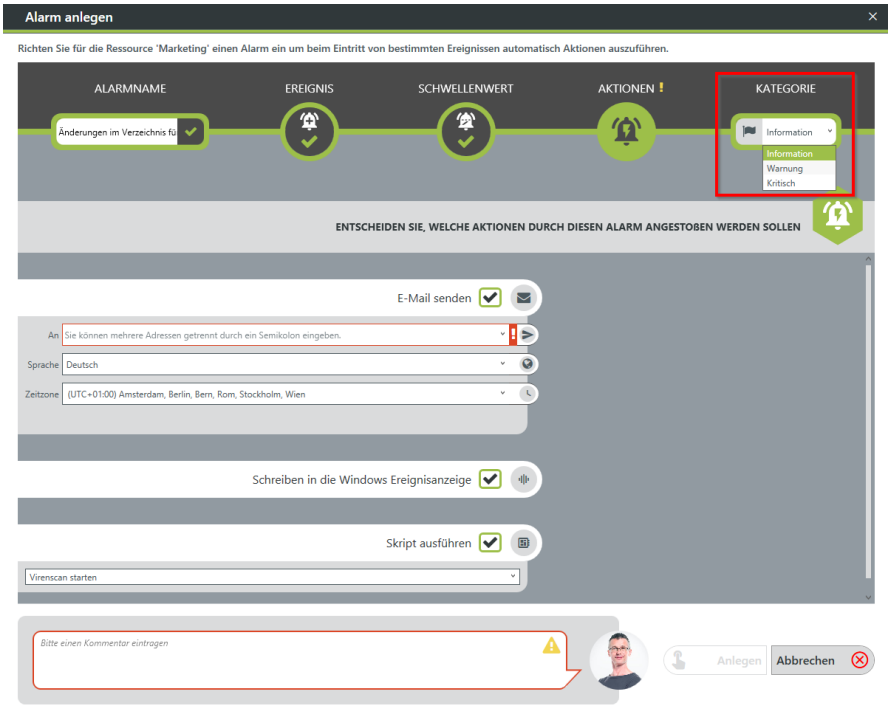
Optional:

Definieren Sie mit Hilfe der Blacklist, welche Verzeichnisse nicht überwacht werden.

1. *Nutzen Sie die Filterfunktion, um die gewünschten Verzeichnisse zu finden. Wenn Sie filtern, ändert sich die Baumansicht zu einer Ergebnisliste der Verzeichnispfade.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Verzeichnisse zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Verzeichnisse von der Blacklist zu entfernen.*
4. *Schalten Sie die Überwachung der Unterverzeichnisse ein oder aus.*
5. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*

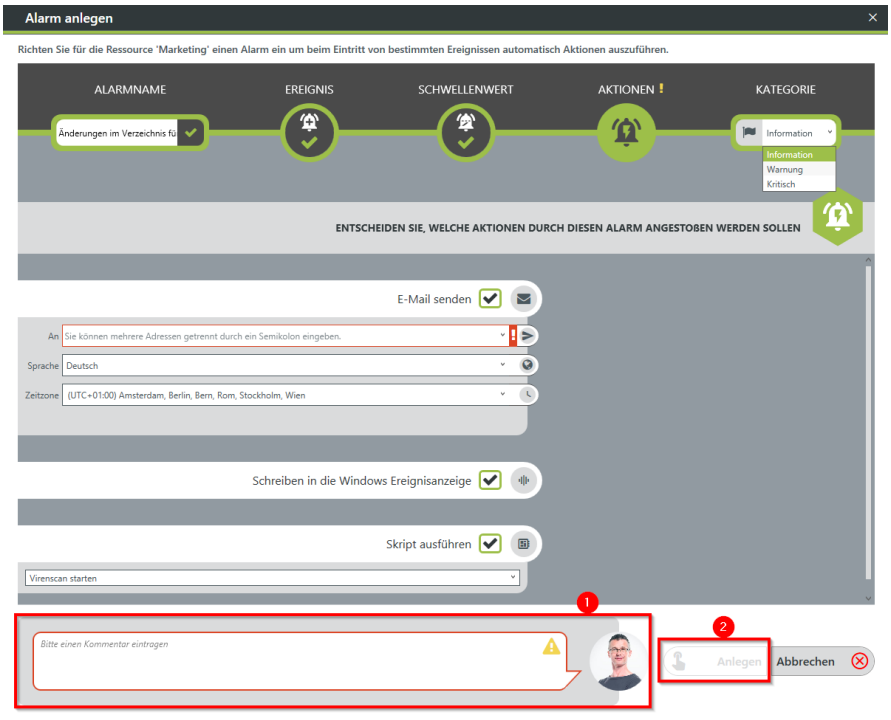


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll.*
   Der Inhalt der E-Mails kann angepasst werden. Dies erfolgt analog zu den Rezertifizierungs-E-Mails.
3. *Der Alarm wird in die Windows Ereignisanzeige geschrieben. Dabei wird die Kategorisierung angewendet. Diese Option ist besonders nützlich, wenn Sie ein SIEM-System einsetzen.*
4. *Aktivieren Sie die Ausführung eines Skripts. Um diese Option aktivieren zu können, muss eine Skriptkonfiguration für Alarme hinterlegt sein.*



Wählen Sie eine Kategorie.

Diese wird beim Schreiben in die Windows Ereignisanzeige und für den E-Mail Betreff verwendet.



1. *Sie müssen eine Begründung für die Alarmkonfiguration angeben, um diese speichern zu können.*
2. *Klicken Sie auf "Anlegen".*

6.2.1.3 Alarme für Verdachtsfälle auf Datendiebstahl aktivieren (Fileserver)

Hintergrund / Mehrwert

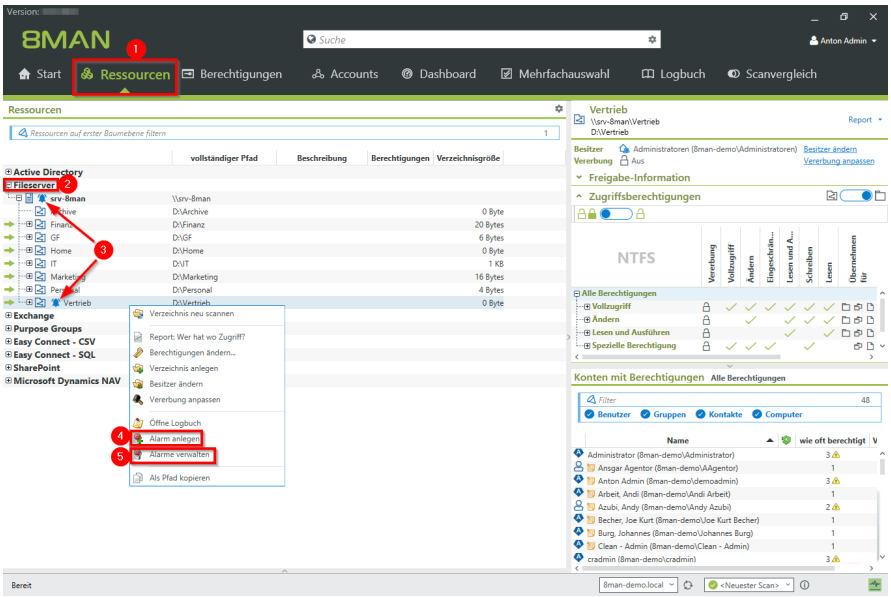
Um Sicherheitsvorfälle effizient zu erfassen, nimmt 8MAN die von Nutzern ausgelösten Fileserver-Events in den Blick. Treten diese in ungewohnt hoher Zahl und zusätzlich in einem kurzen Zeitraum auf, informiert 8MAN proaktiv alle Verantwortlichen.

Datendiebstahl: Ein Nutzerkonto liest in einem kurzen Zeitraum ungewöhnlich viele Dateien ein („File read“)

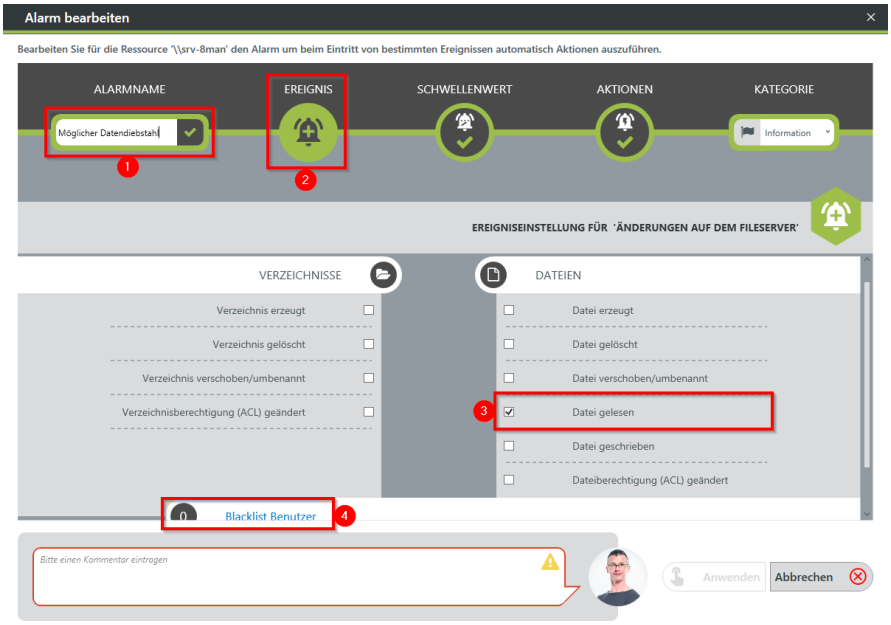
Weiterführende Services

Alarme für Fileserververzeichnisse aktivieren
Alarme für Datenlöschungen aktivieren (Fileserver)
Alarme für Verdachtsfälle auf Ransomware aktivieren (Fileserver)
Nach einem Alarm ein Skript ausführen
Alarme verwalten

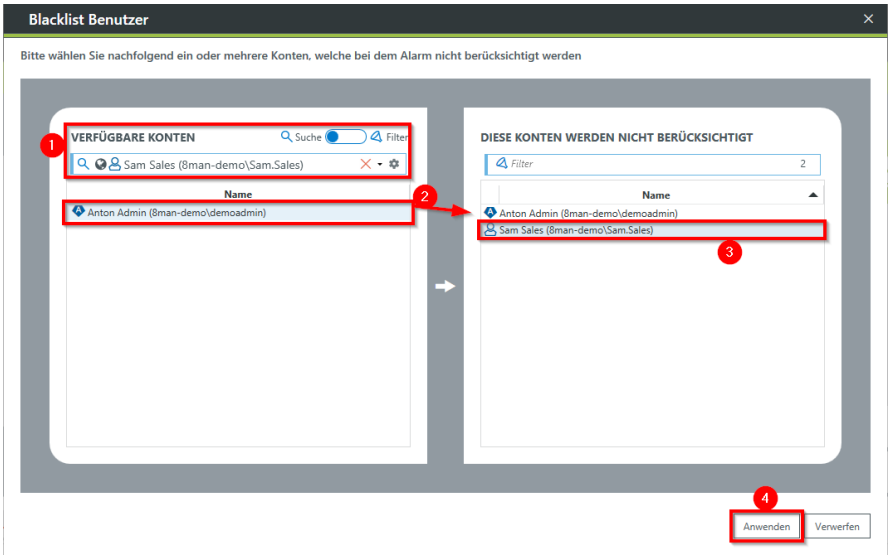
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Expandieren Sie den "Fileserver".*
3. *Bereits eingerichtete Alarme werden mit einem Glockensymbol dargestellt.*
4. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarm anlegen" im Kontextmenü, um einen neuen Alarm anzulegen.*
5. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarme verwalten" im Kontextmenü, um bestehende Alarme anzupassen oder zu löschen.*



1. *Geben Sie der Alarmkonfiguration einen Namen.*
2. *Wählen Sie "Ereignis".*
3. *Legen Sie fest, welche Ereignisse einen Alarm auslösen. Bei Verdacht auf Datendiebstahl typisch: "Datei gelesen".*
4. *Klicken Sie auf "Blacklist Benutzer".*



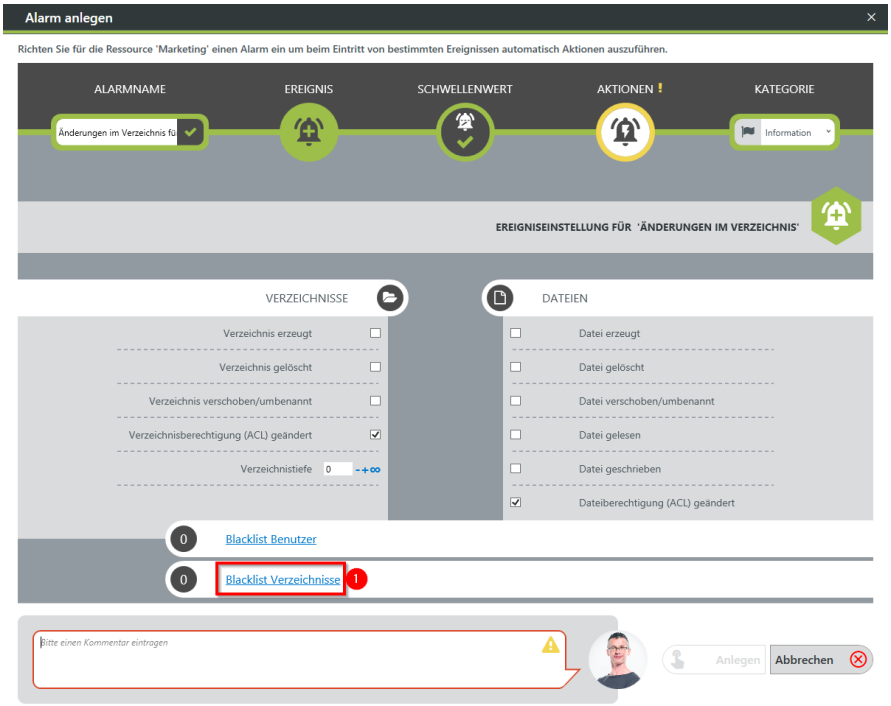
Optional:

Definieren Sie mit Hilfe der Blacklist, welche Benutzer keinen Alarm auslösen.

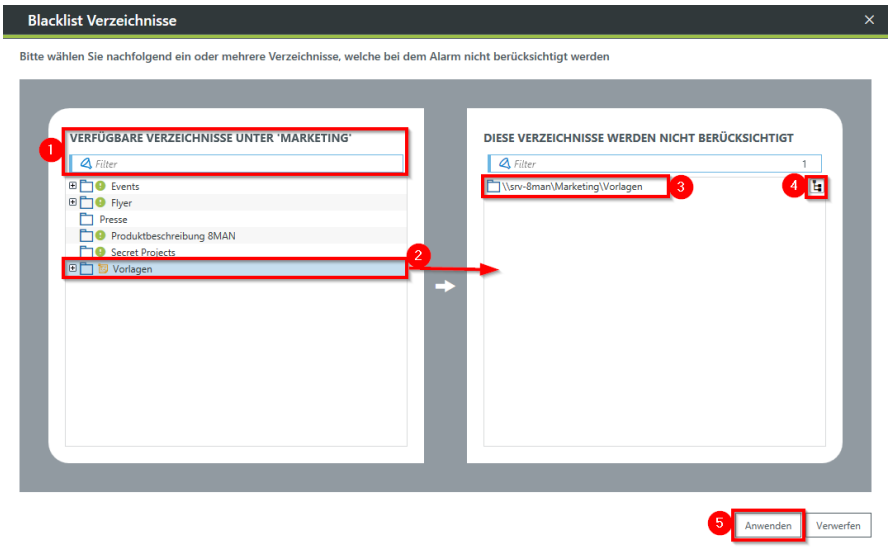
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

Sie können nur Benutzer hinzufügen, keine Gruppen.

1. *Nutzen Sie die Suchfunktion, um die gewünschten Benutzer zu finden.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Benutzer zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Benutzer von der Blacklist zu entfernen.*
4. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*



1. *Wählen Sie "Blacklist Verzeichnisse".*

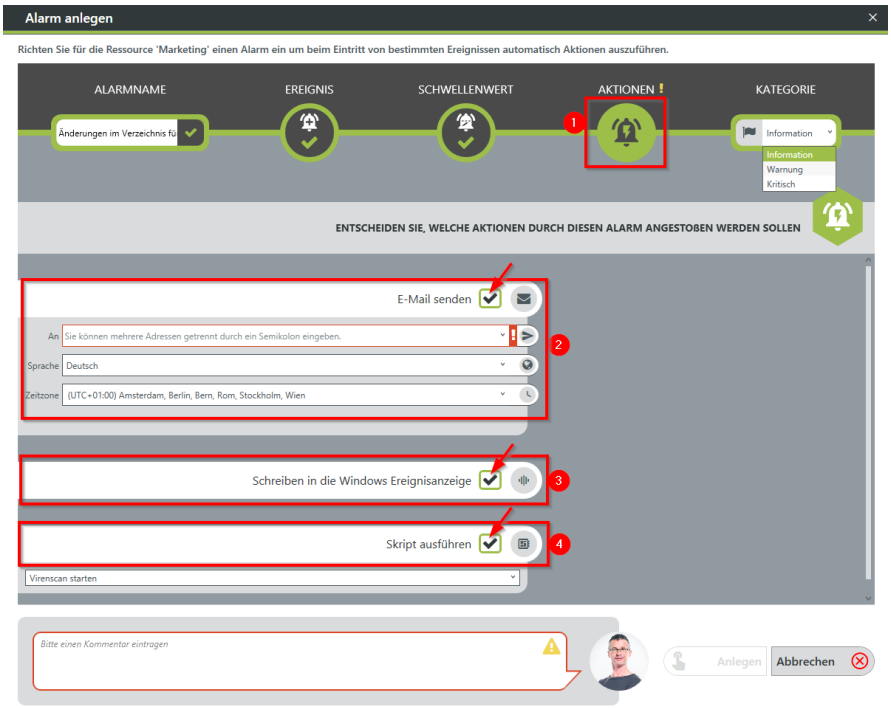


Optional:

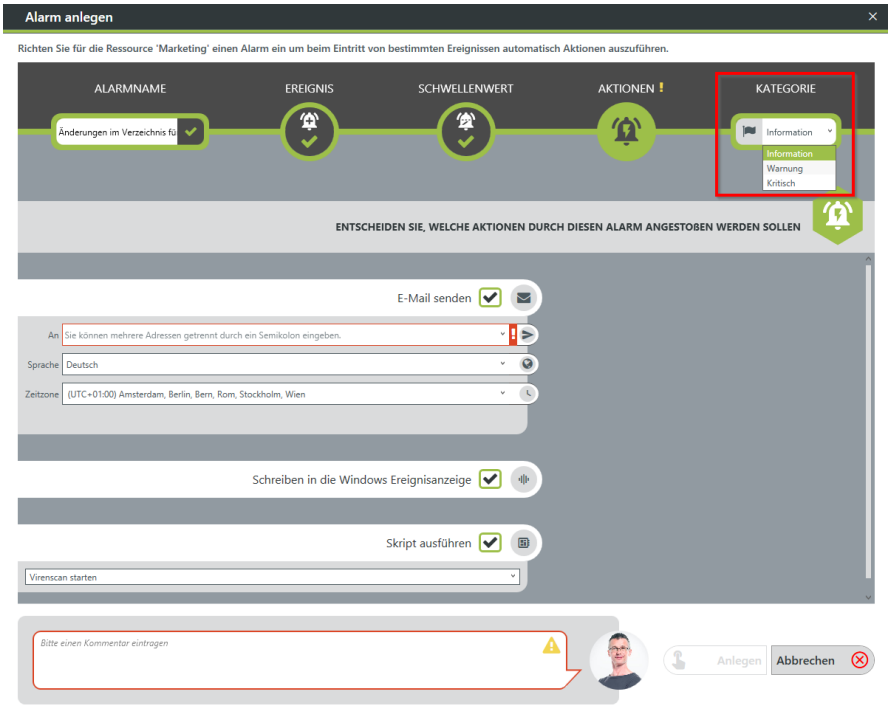
Definieren Sie mit Hilfe der Blacklist, welche Verzeichnisse nicht überwacht werden.

1. *Nutzen Sie die Filterfunktion, um die gewünschten Verzeichnisse zu finden. Wenn Sie filtern, ändert sich die Baumansicht zu einer Ergebnisliste der Verzeichnispfade.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Verzeichnisse zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Verzeichnisse von der Blacklist zu entfernen.*
4. *Schalten Sie die Überwachung der Unterverzeichnisse ein oder aus.*
5. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*

1. *Wählen Sie "Schwellenwert".*
2. *Aktivieren Sie Schwellenwert.*
3. *Aktivieren Sie die Option. Bei einem Verdacht auf Datendiebstahl werden wahrscheinlich alle Ereignisse von einem Benutzer ausgelöst.*
4. *Legen Sie fest, wieviele Ereignisse innerhalb eines Zeitraumes den Alarm auslösen.*

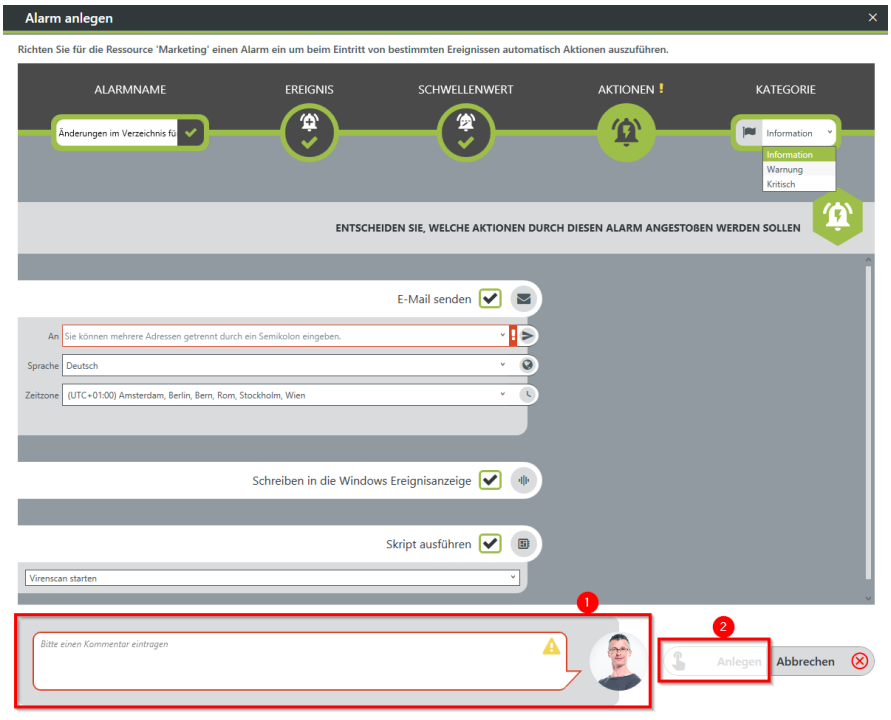


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll.*
   Der Inhalt der E-Mails kann angepasst werden. Dies erfolgt analog zu den Rezertifizierungs-E-Mails.
3. *Der Alarm wird in die Windows Ereignisanzeige geschrieben. Dabei wird die Kategorisierung angewendet. Diese Option ist besonders nützlich, wenn Sie ein SIEM-System einsetzen.*
4. *Aktivieren Sie die Ausführung eines Skripts. Um diese Option aktivieren zu können, muss eine Skriptkonfiguration für Alarme hinterlegt sein.*



Wählen Sie eine Kategorie.

Diese wird beim Schreiben in die Windows Ereignisanzeige und für den E-Mail Betreff verwendet.



1. *Sie müssen eine Begründung für die Alarmkonfiguration angeben, um diese speichern zu können.*
2. *Klicken Sie auf "Anlegen".*

6.2.1.4 Alarme für Datenlöschungen aktivieren (Fileserver)

Hintergrund / Mehrwert

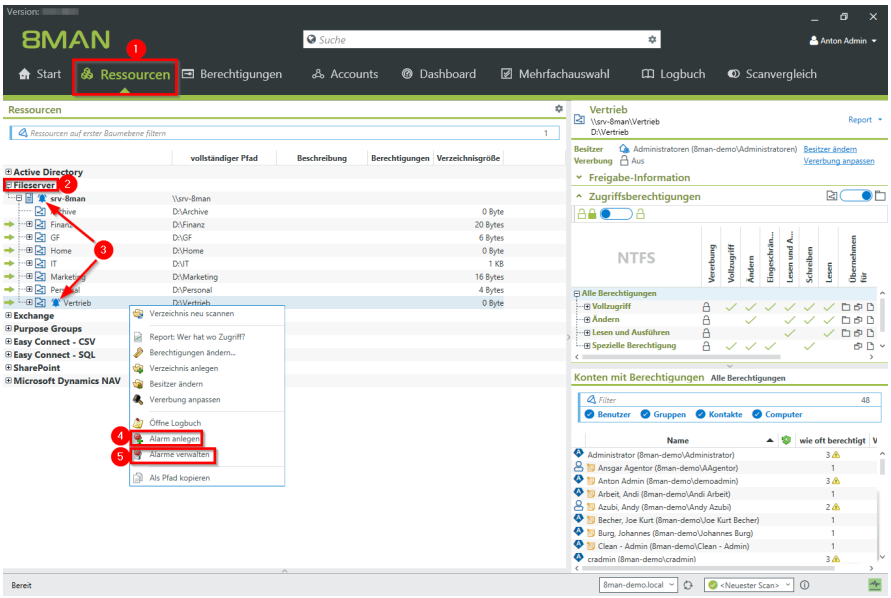
Um Sicherheitsvorfälle effizient zu erfassen, nimmt 8MAN die von Nutzern ausgelösten Fileserver-Events in den Blick. Treten diese in ungewohnt hoher Zahl und zusätzlich in einem kurzen Zeitraum auf, informiert 8MAN proaktiv alle Verantwortlichen.

Datenlöschungen: Ein Nutzerkonto löscht in einem kurzen Zeitraum sehr viele Dateien („File delete“)

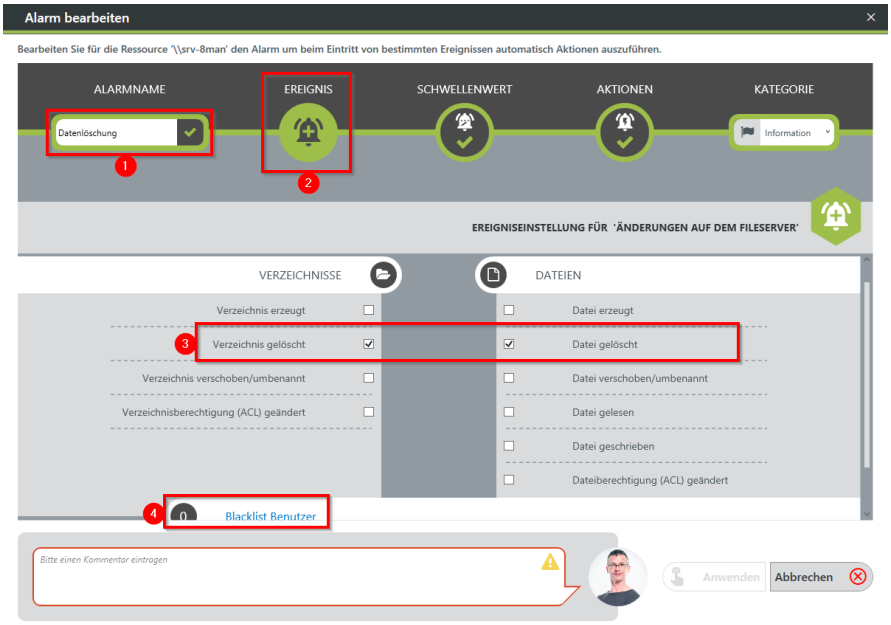
Weiterführende Services

Alarme für Fileserververzeichnisse aktivieren
Alarme für Verdachtsfälle auf Datendiebstahl aktivieren (Fileserver)
Alarme für Verdachtsfälle auf Ransomware aktivieren (Fileserver)
Nach einem Alarm ein Skript ausführen
Alarme verwalten

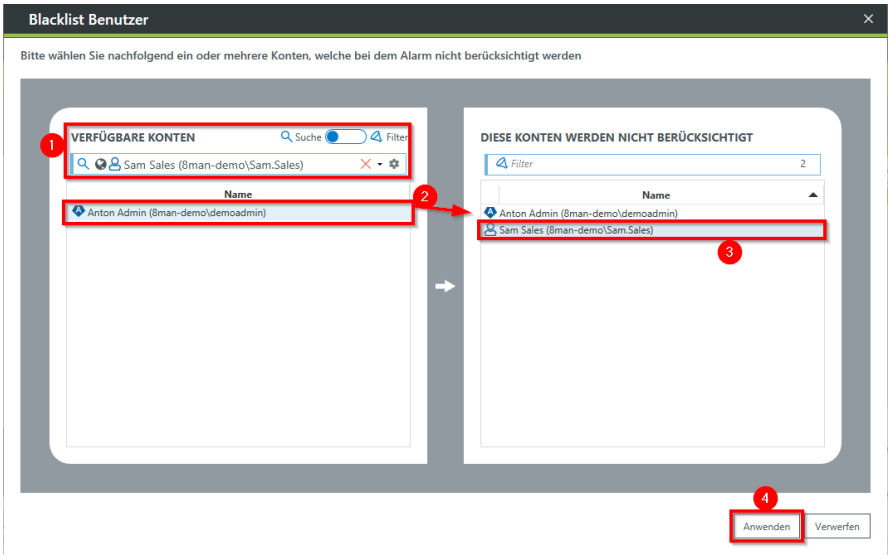
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Expandieren Sie den "Fileserver".*
3. *Bereits eingerichtete Alarme werden mit einem Glockensymbol dargestellt.*
4. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarm anlegen" im Kontextmenü, um einen neuen Alarm anzulegen.*
5. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarme verwalten" im Kontextmenü, um bestehende Alarme anzupassen oder zu löschen.*



1. *Geben Sie der Alarmkonfiguration einen Namen.*
2. *Wählen Sie "Ereignis".*
3. *Legen Sie fest, welche Ereignisse einen Alarm auslösen. Bei Datenlöschungen typisch: "Verzeichnis gelöscht" und "Datei gelöscht".*
4. *Klicken Sie auf "Blacklist Benutzer".*



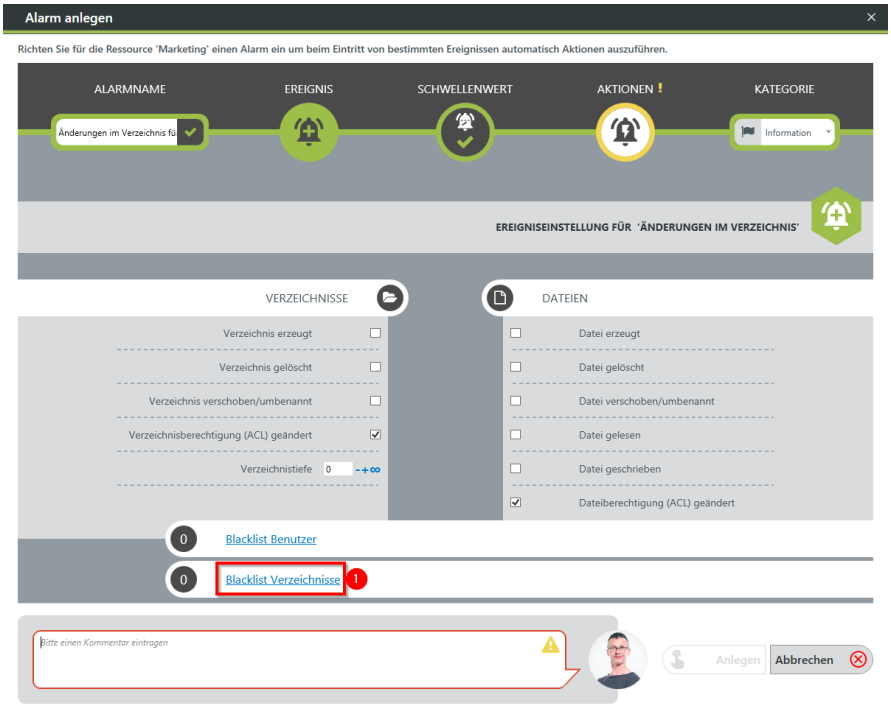
Optional:

Definieren Sie mit Hilfe der Blacklist, welche Benutzer keinen Alarm auslösen.

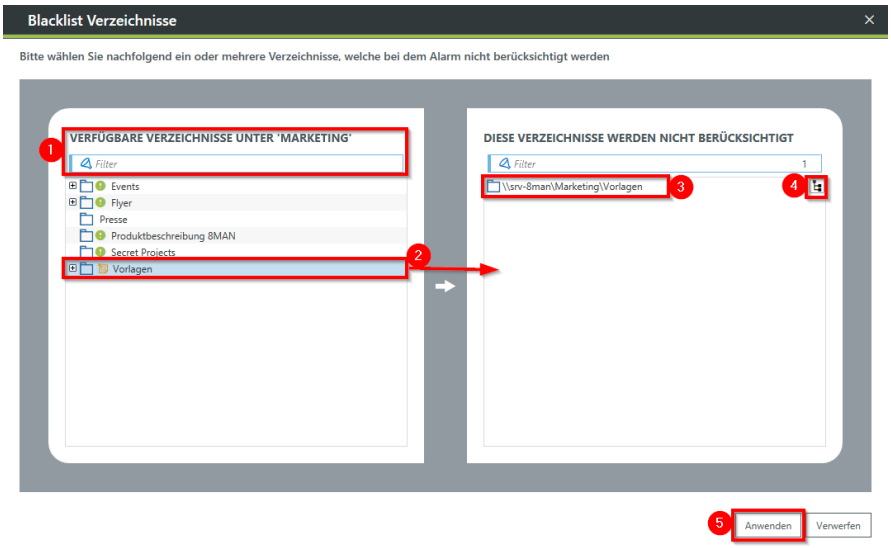
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

Sie können nur Benutzer hinzufügen, keine Gruppen.

1. *Nutzen Sie die Suchfunktion, um die gewünschten Benutzer zu finden.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Benutzer zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Benutzer von der Blacklist zu entfernen.*
4. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*



1. *Wählen Sie "Blacklist Verzeichnisse".*

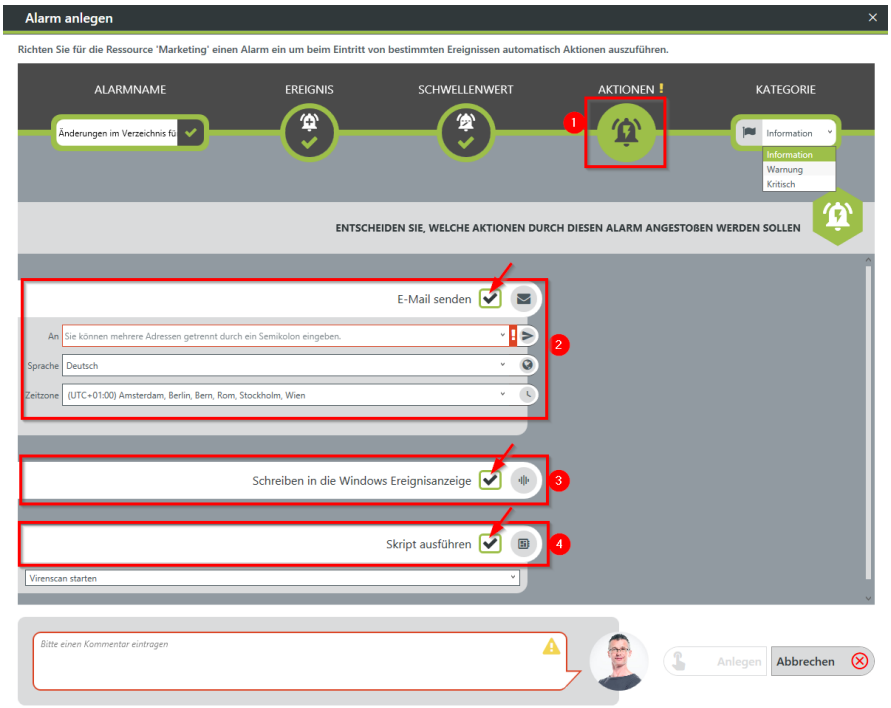


Optional:

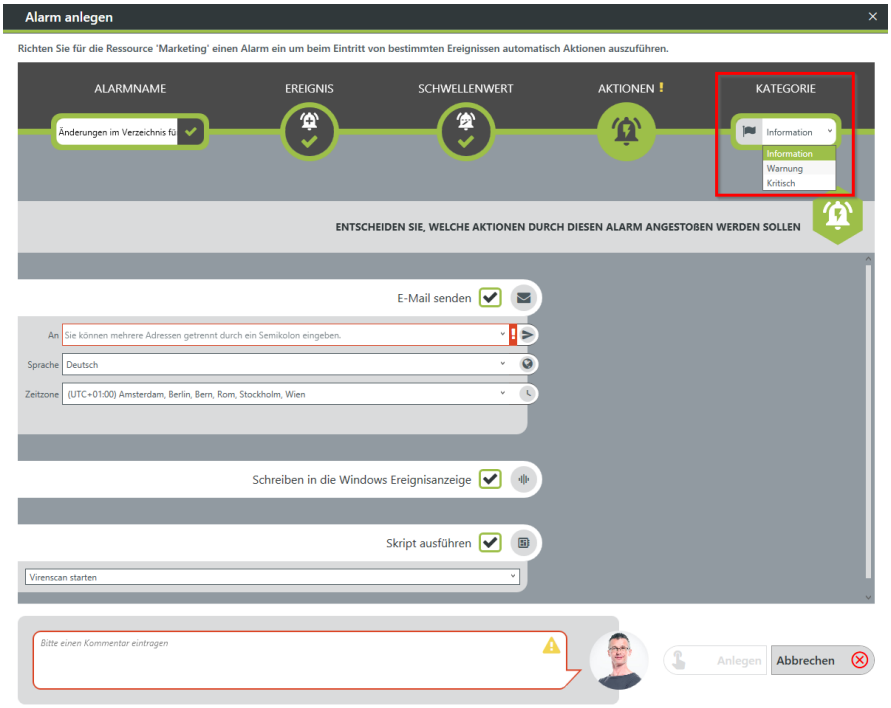
Definieren Sie mit Hilfe der Blacklist, welche Verzeichnisse nicht überwacht werden.

1. *Nutzen Sie die Filterfunktion, um die gewünschten Verzeichnisse zu finden. Wenn Sie filtern, ändert sich die Baumansicht zu einer Ergebnisliste der Verzeichnispfade.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Verzeichnisse zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Verzeichnisse von der Blacklist zu entfernen.*
4. *Schalten Sie die Überwachung der Unterverzeichnisse ein oder aus.*
5. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*

1. *Wählen Sie "Schwellenwert".*
2. *Aktivieren Sie Schwellenwert.*
3. *Aktivieren Sie die Option.*
4. *Legen Sie fest, wieviele Ereignisse innerhalb eines Zeitraumes den Alarm auslösen.*

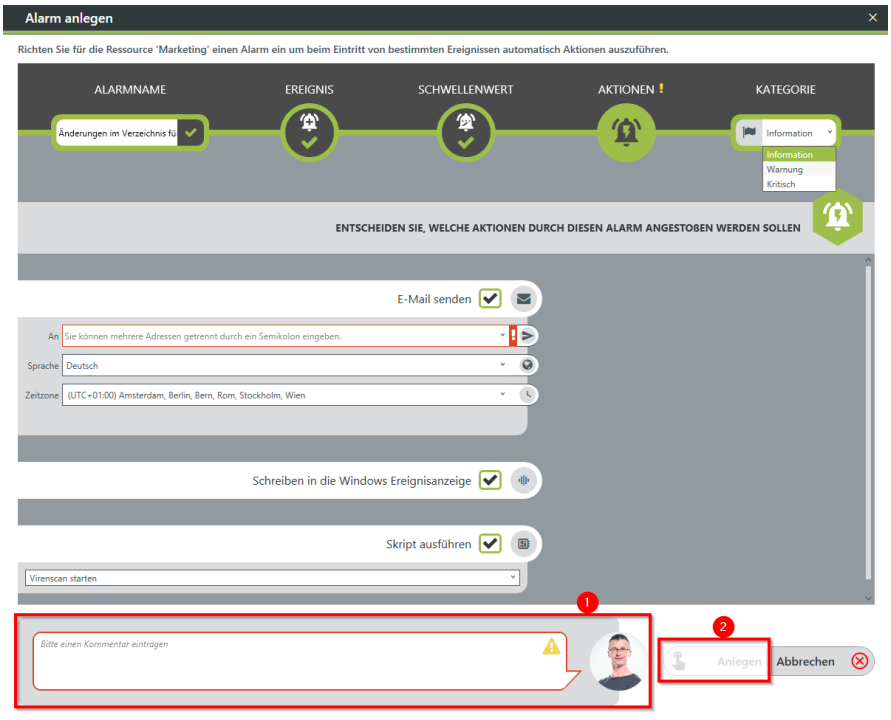


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll.*
   Der Inhalt der E-Mails kann angepasst werden. Dies erfolgt analog zu den Rezertifizierungs-E-Mails.
3. *Der Alarm wird in die Windows Ereignisanzeige geschrieben. Dabei wird die Kategorisierung angewendet. Diese Option ist besonders nützlich, wenn Sie ein SIEM-System einsetzen.*
4. *Aktivieren Sie die Ausführung eines Skripts. Um diese Option aktivieren zu können, muss eine Skriptkonfiguration für Alarme hinterlegt sein.*



Wählen Sie eine Kategorie.

Diese wird beim Schreiben in die Windows Ereignisanzeige und für den E-Mail Betreff verwendet.



1. *Sie müssen eine Begründung für die Alarmkonfiguration angeben, um diese speichern zu können.*
2. *Klicken Sie auf "Anlegen".*

6.2.1.5 Alarme für Verdachtsfälle auf Ransomware aktivieren (Fileserver)

Hintergrund / Mehrwert

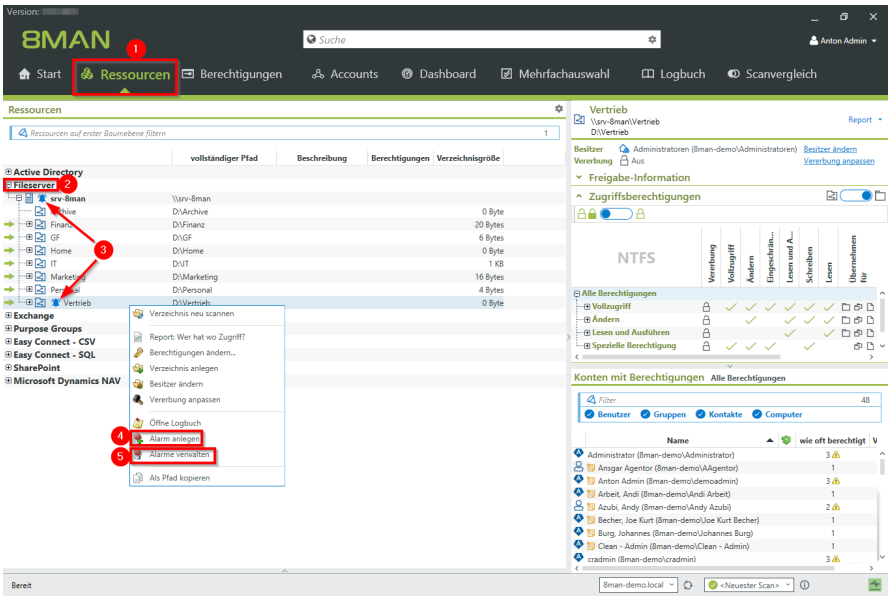
Um Sicherheitsvorfälle effizient zu erfassen, nimmt 8MAN die von Nutzern ausgelösten Fileserver-Events in den Blick. Treten diese in ungewohnt hoher Zahl und zusätzlich in einem kurzen Zeitraum auf, informiert 8MAN proaktiv alle Verantwortlichen.

Ransomware Attacke: Von einem Nutzerkonto geht die Kombination aus Dateierstellung und Löschung aus („File create“ & „File delete“)

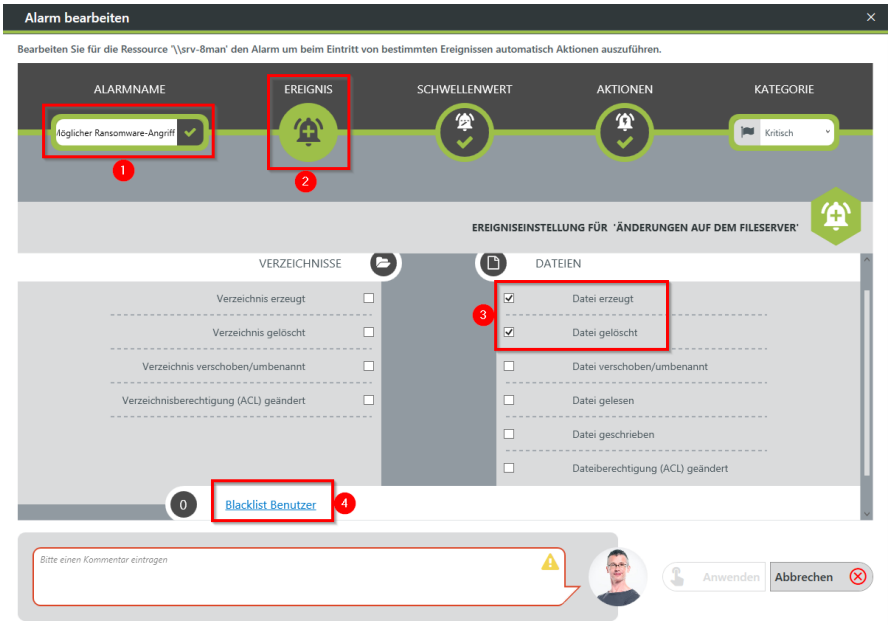
Weiterführende Services

Alarme für Fileserververzeichnisse aktivieren
Alarme für Verdachtsfälle auf Datendiebstahl aktivieren (Fileserver)
Alarme für Datenlöschungen aktivieren (Fileserver)
Nach einem Alarm ein Skript ausführen
Alarme verwalten

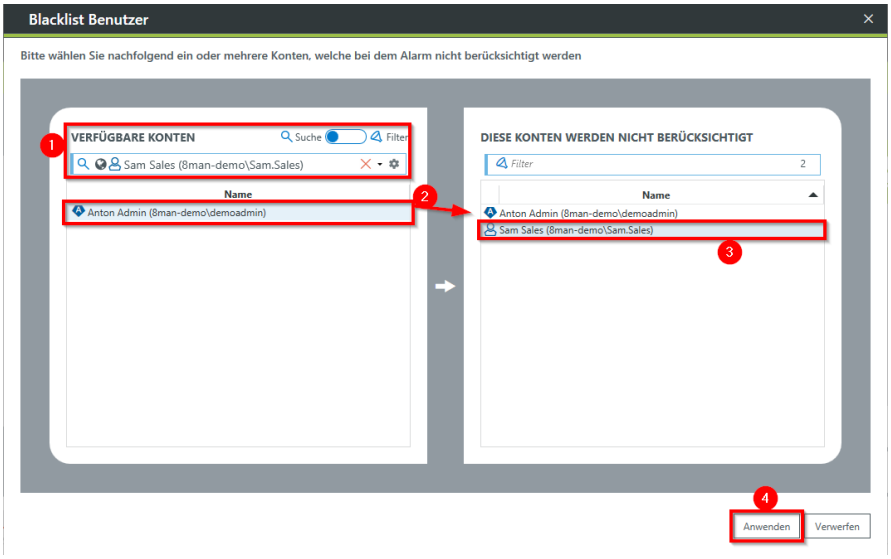
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Expandieren Sie den "Fileserver".*
3. *Bereits eingerichtete Alarme werden mit einem Glockensymbol dargestellt.*
4. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarm anlegen" im Kontextmenü, um einen neuen Alarm anzulegen.*
5. *Rechtsklicken Sie eine Ressource und wählen Sie "Alarme verwalten" im Kontextmenü, um bestehende Alarme anzupassen oder zu löschen.*



1. *Geben Sie der Alarmkonfiguration einen Namen.*
2. *Wählen Sie "Ereignis".*
3. *Legen Sie fest, welche Ereignisse einen Alarm auslösen. Bei Ransomware typisch: "Datei erzeugt" und "Datei gelöscht".*
4. *Klicken Sie auf "Blacklist Benutzer".*



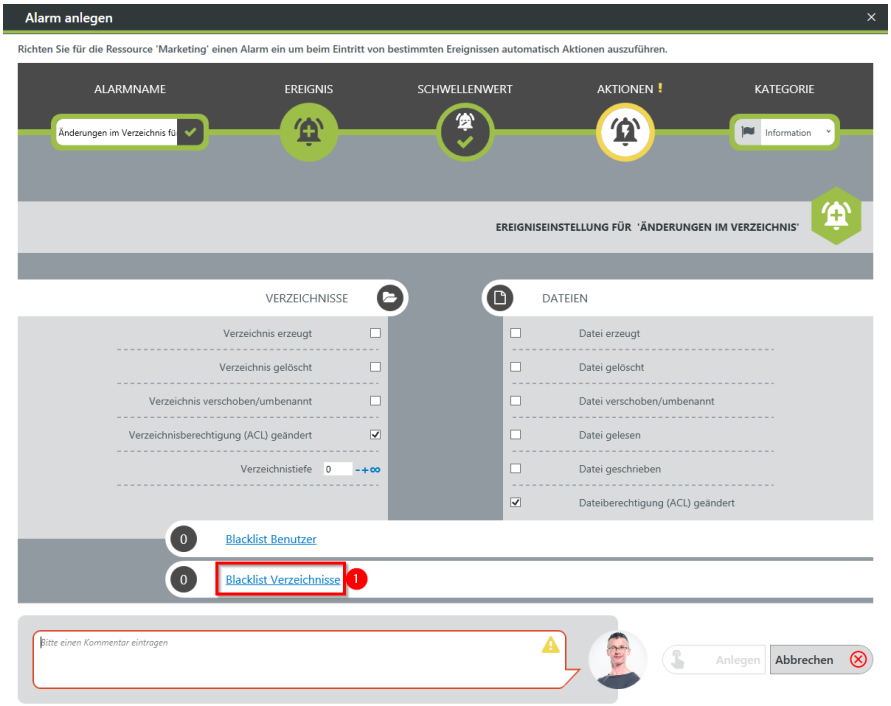
Optional:

Definieren Sie mit Hilfe der Blacklist, welche Benutzer keinen Alarm auslösen.

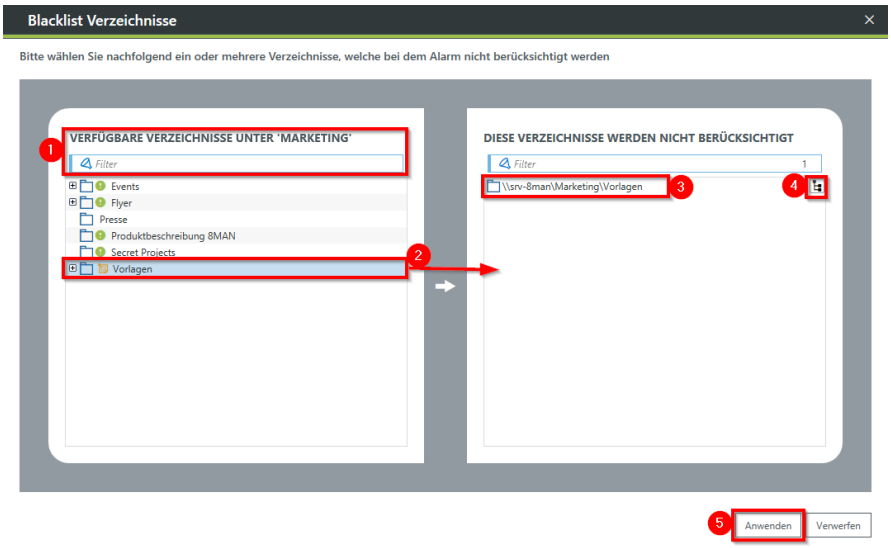
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

Sie können nur Benutzer hinzufügen, keine Gruppen.

1. *Nutzen Sie die Suchfunktion, um die gewünschten Benutzer zu finden.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Benutzer zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Benutzer von der Blacklist zu entfernen.*
4. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*



1. *Wählen Sie "Blacklist Verzeichnisse".*

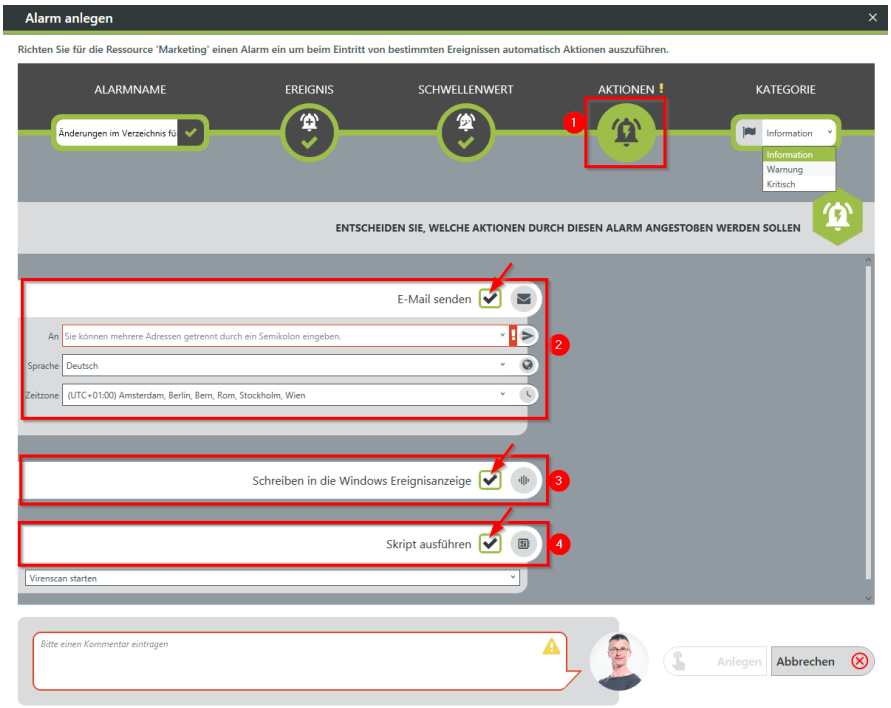


Optional:

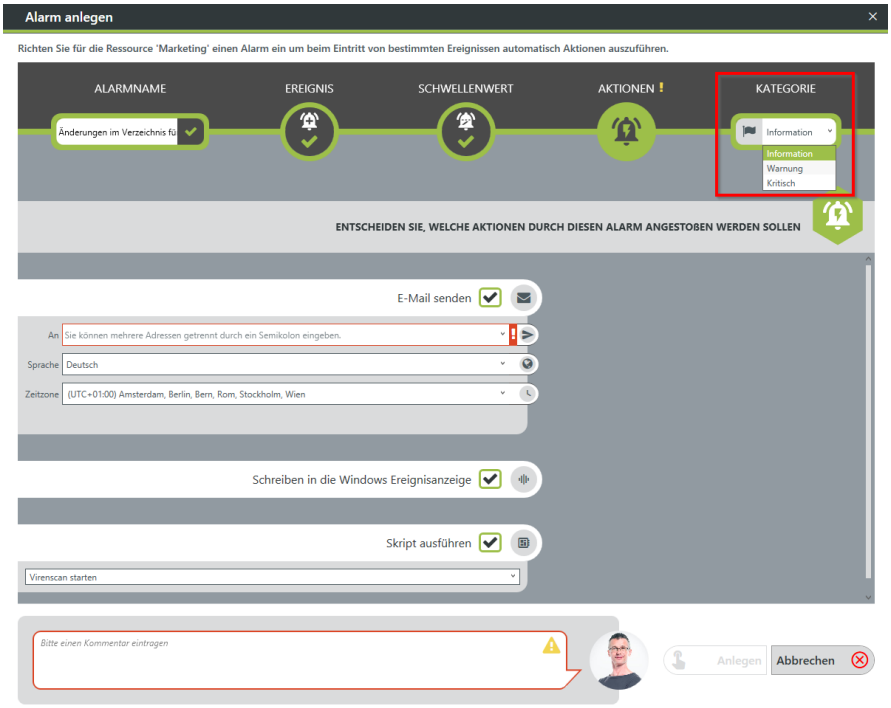
Definieren Sie mit Hilfe der Blacklist, welche Verzeichnisse nicht überwacht werden.

1. *Nutzen Sie die Filterfunktion, um die gewünschten Verzeichnisse zu finden. Wenn Sie filtern, ändert sich die Baumansicht zu einer Ergebnisliste der Verzeichnispfade.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Verzeichnisse zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Verzeichnisse von der Blacklist zu entfernen.*
4. *Schalten Sie die Überwachung der Unterverzeichnisse ein oder aus.*
5. *Klicken Sie auf "Anwenden", um die Änderungen zu speichern.*

1. *Wählen Sie "Schwellenwert".*
2. *Aktivieren Sie Schwellenwert.*
3. *Aktivieren Sie die Option. Bei einem Verdacht auf Ransomware werden typischerweise alle Ereignisse von einem Benutzer ausgelöst.*
4. *Legen Sie fest, wieviele Ereignisse innerhalb eines Zeitraumes den Alarm auslösen.*

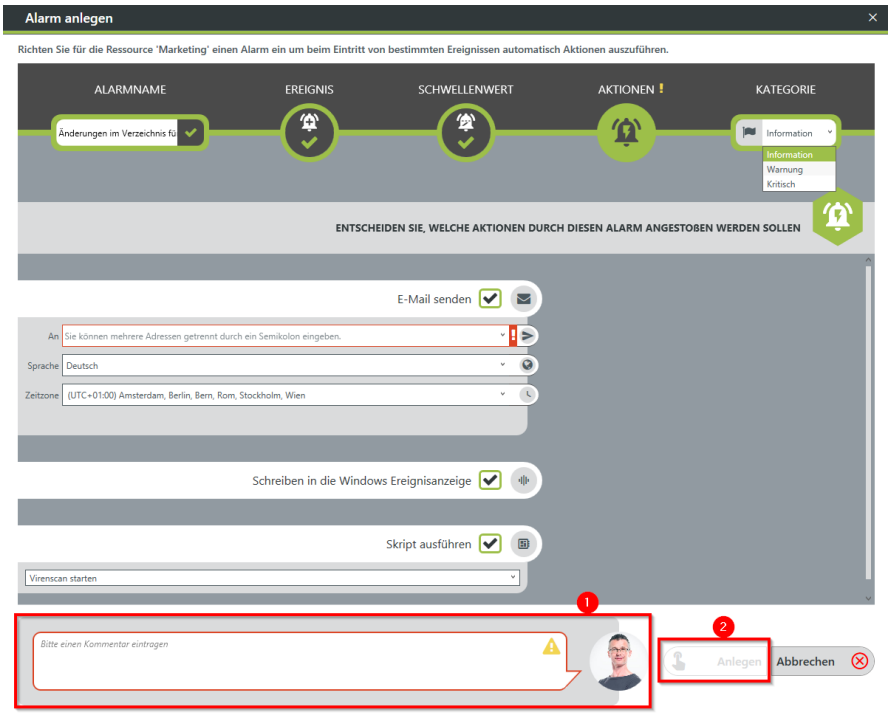


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll.*
   Der Inhalt der E-Mails kann angepasst werden. Dies erfolgt analog zu den Rezertifizierungs-E-Mails.
3. *Der Alarm wird in die Windows Ereignisanzeige geschrieben. Dabei wird die Kategorisierung angewendet. Diese Option ist besonders nützlich, wenn Sie ein SIEM-System einsetzen.*
4. *Aktivieren Sie die Ausführung eines Skripts. Um diese Option aktivieren zu können, muss eine Skriptkonfiguration für Alarme hinterlegt sein.*



Wählen Sie eine Kategorie.

Diese wird beim Schreiben in die Windows Ereignisanzeige und für den E-Mail Betreff verwendet.



1. *Sie müssen eine Begründung für die Alarmkonfiguration angeben, um diese speichern zu können.*
2. *Klicken Sie auf "Anlegen".*

6.3 Exchange

6.3.1 +8MATE Exchange Logga: Aktivitäten an Postfächern überwachen

Hintergrund / Mehrwert

Microsoft Exchange dient der zentralen Ablage und Verwaltung von E-Mails, Terminen, Kontakten und Aufgaben. Als zentrale Lösung für unternehmensweite Kollaboration ist nicht nur die Frage nach Zugriffsrechten relevant, sondern auch ein Monitoring der tatsächlich ausgeführten Aktivitäten.

Der 8MATE Exchange Logga protokolliert Aktivitäten von Postfach-Besitzern, ihren Stellvertretern und Administratoren.

Besonders sicherheitskritisch sind dabei die folgenden Aktionen:

- Hard Delete: Wer hat E-Mails, Kontakte oder Kalendereinträge vom Exchange Server gelöscht?
- MessageBind: Hat ein Mitarbeiter aus der IT in meine E-Mails geschaut?
- SendAs: Wer hat wann im Namen meiner Person E-Mails versendet?
- SendOnBehalf: Wer hat wann in meinem Auftrag E-Mails versendet?
- SoftDelete: Wer (außer mir) hat E-Mails in meinem Postfach gelöscht?

Services

Aktivitäten an Postfächern, Kalendern und Kontakten überwachen (Report)
Aktivitäten in Postfächern, Kalendern und Kontakten anzeigen (Logbuch)

6.3.1.1 Aktivitäten an Postfächern, Kalendern und Kontakten überwachen (Report)

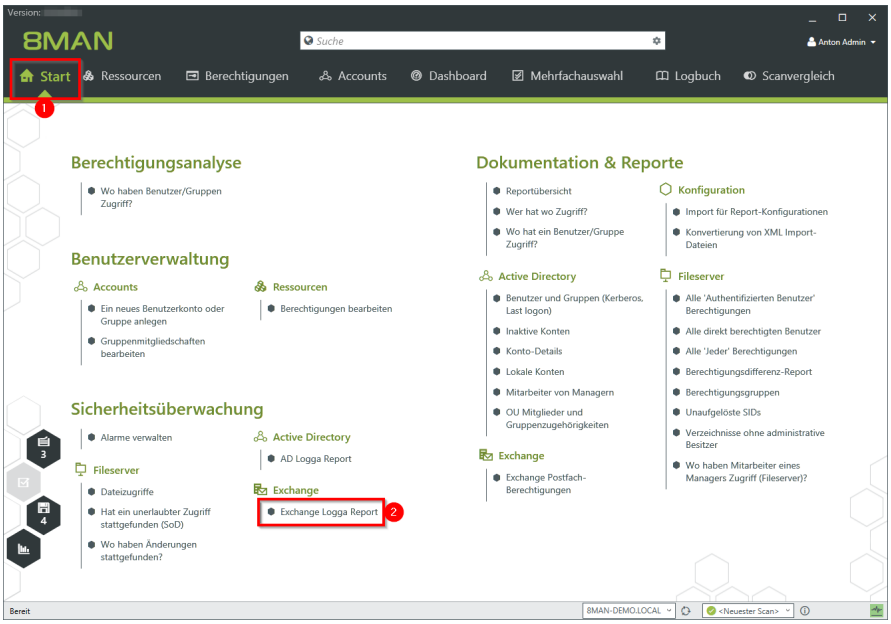
Hintergrund / Mehrwert

Mit dem 8MATE Exchange Logga aufgezeichnete Ereignisse können Sie mit den Reportfunktionen detailliert und wiederkehrend analysieren. Schneller beantworten Sie konkrete Fragen zu Exchange-Aktivitäten mit der Logbuchansicht.

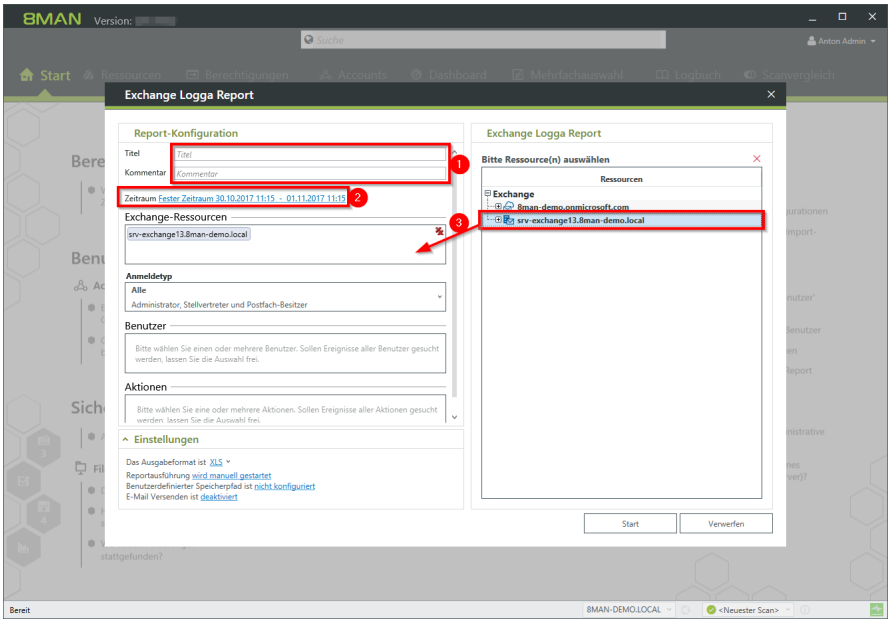
Weiterführende Services

Aktivitäten in Postfächern, Kalendern und Kontakten anzeigen (Logbuch)

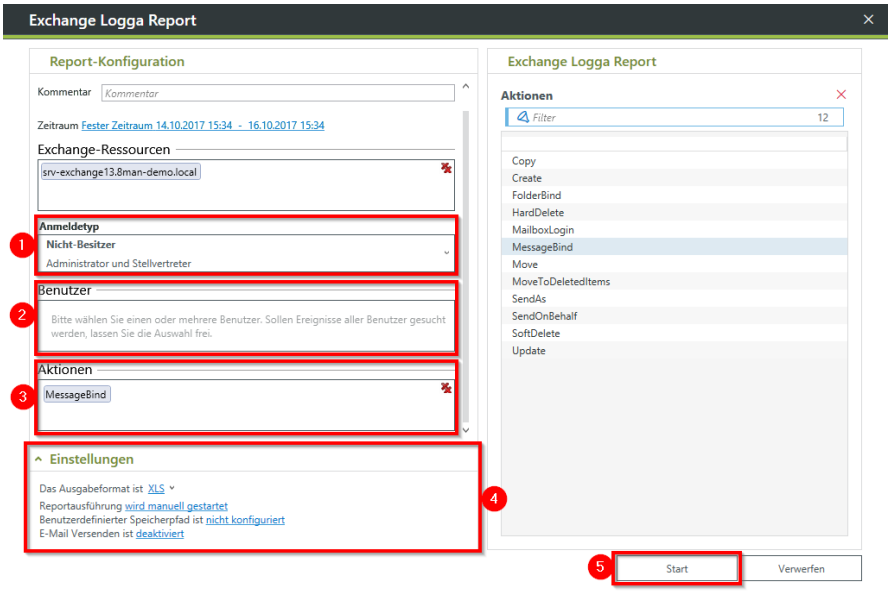
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Exchange Logga Report".*



1. *Optional: Geben Sie dem Report einen Titel und eine Beschreibung.*
2. *Legen Sie den Zeitraum fest.*
3. *Fügen Sie die gewünschten Ressourcen per Drag&Drop hinzu.*



1. *Wählen Sie den Anmeldetyp aus.*
2. *Haben Sie spezielle Benutzer im Fokus, fügen Sie diese per Drag&Drop hinzu. Für alle Benutzer lassen Sie die Auswahl frei.*
3. *Optional: Wählen Sie Aktionen aus.*
4. *Legen Sie Ausgabeoptionen für den Report fest.*
5. *Starten Sie die Ausführung.*

6.3.1.2 Aktivitäten in Postfächern, Kalendern und Kontakten anzeigen (Logbuch)

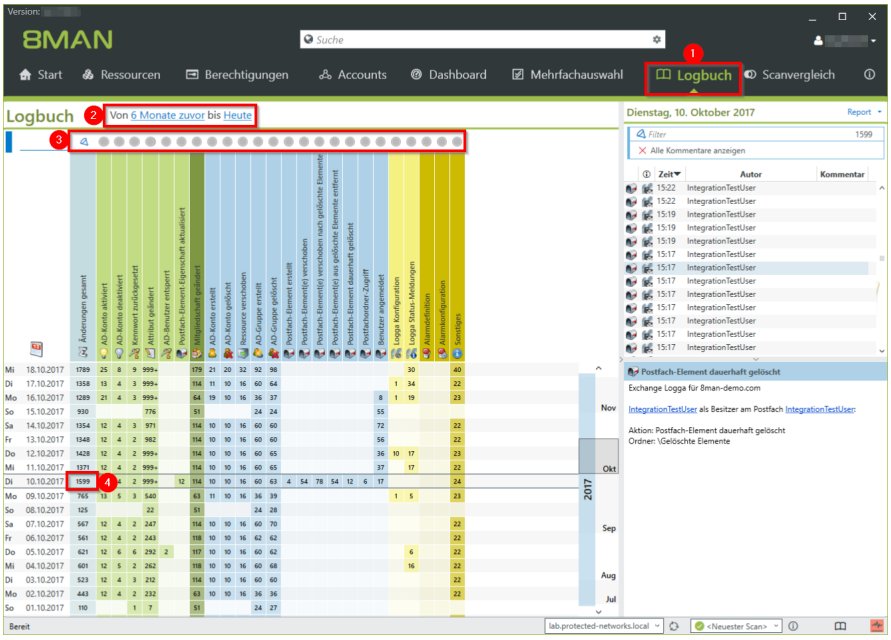
Hintergrund / Mehrwert

Mit dem 8MATE Exchange Logga aufgezeichnete Ereignisse können Sie mit den Reportfunktionen detailliert und wiederkehrend analysieren. Schneller beantworten Sie konkrete Fragen zu Exchange-Änderungen mit der Logbuchansicht.

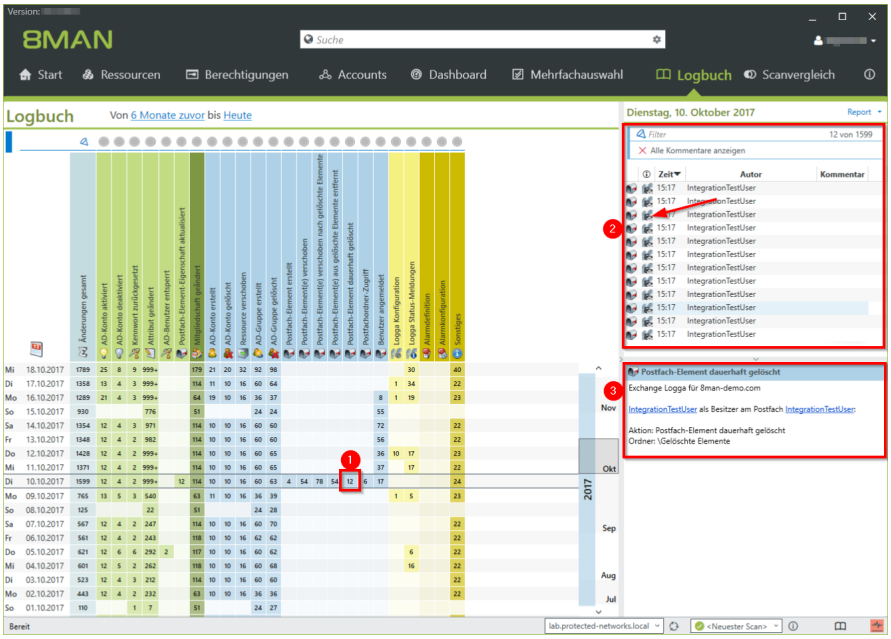
Weiterführende Services

Einen Report über Aktivitäten an Postfächern, Kalendern und Kontakten erstellen

Der Prozess in einzelnen Schritten

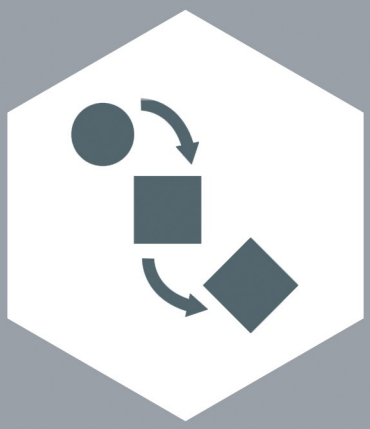


1. *Wählen Sie "Logbuch".*
2. *Legen Sie den Zeitraum für die Logbuch-Analyse fest.*
3. *Über die Filter fokussieren Sie auf die Events, die Sie prüfen möchten.*
4. *Selektieren Sie alle Ereignisse eines Tages (eine Zeile).*



1. *Selektieren Sie eine Zelle (einen Ereignistyp), um Ihre Abfrage weiter einzugrenzen.*
2. *8MAN zeigt eine Liste aller gewählten Ereignisse. An dem "Fußspuren-Symbol mit Briefumschlag" erkennen Sie vom Exchange Logga aufgezeichnete Ereignisse. Selektieren Sie ein Ereignis.*
3. *8MAN zeigt alle Details zum Ereignis.*

7. Role & Process Optimization



7.1 Delegation von Aufgaben (Administrator)

8MAN verfügt über Funktionen, die nicht nur für Administratoren interessant sind.

Je nach Unternehmensgröße, Sicherheitsbedarf und vorhandener Prozesse, kann 8MAN von unterschiedlichen Rollen genutzt werden.
Hier ein idealtypisches Schaubild:

Unternehmensgröße in Mitarbeitern	IT Leiter / Auditor / Datenschützer	Administrator	Data Owner (Führungskraft)	Helpdesk
50+	Sichtung der Reporte	Übernahme aller Aktivitäten mit 8MAN		
500+	Sichtung der Reporte	Analyse der gesamten Berechtigungssituation, Useranlage, Administration von Nutzerkonten und Gruppen	Analyse und Administration von Berechtigungen eigener Mitarbeiter auf Fileserver-Verzeichnisse.	
>5.000	Sichtung der Reporte	Analyse der gesamten Berechtigungssituation und Administration der AD Gruppen	Analyse und Administration von Berechtigungen eigener Mitarbeiter auf Fileserver-Verzeichnisse.	Standardisierte Useranlage und kontinuierliches Kontomanagement

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements .

7.1.1 Einer Sicherheitsrolle die Analyse der Berechtigungssituation ermöglichen

Hintergrund / Mehrwert

Sie können Auditoren und Datenschützer über zwei Möglichkeiten in Sicherheitsprozesse involvieren:

- Sie geben der Person einen einfachen Lesezugriff in 8MAN.
- Sie definieren zusammen welche Reporte interessant sind und 8MAN versendet diese automatisch im vereinbarten Turnus.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.5 Aufgabenverteilung und Funktionstrennung.

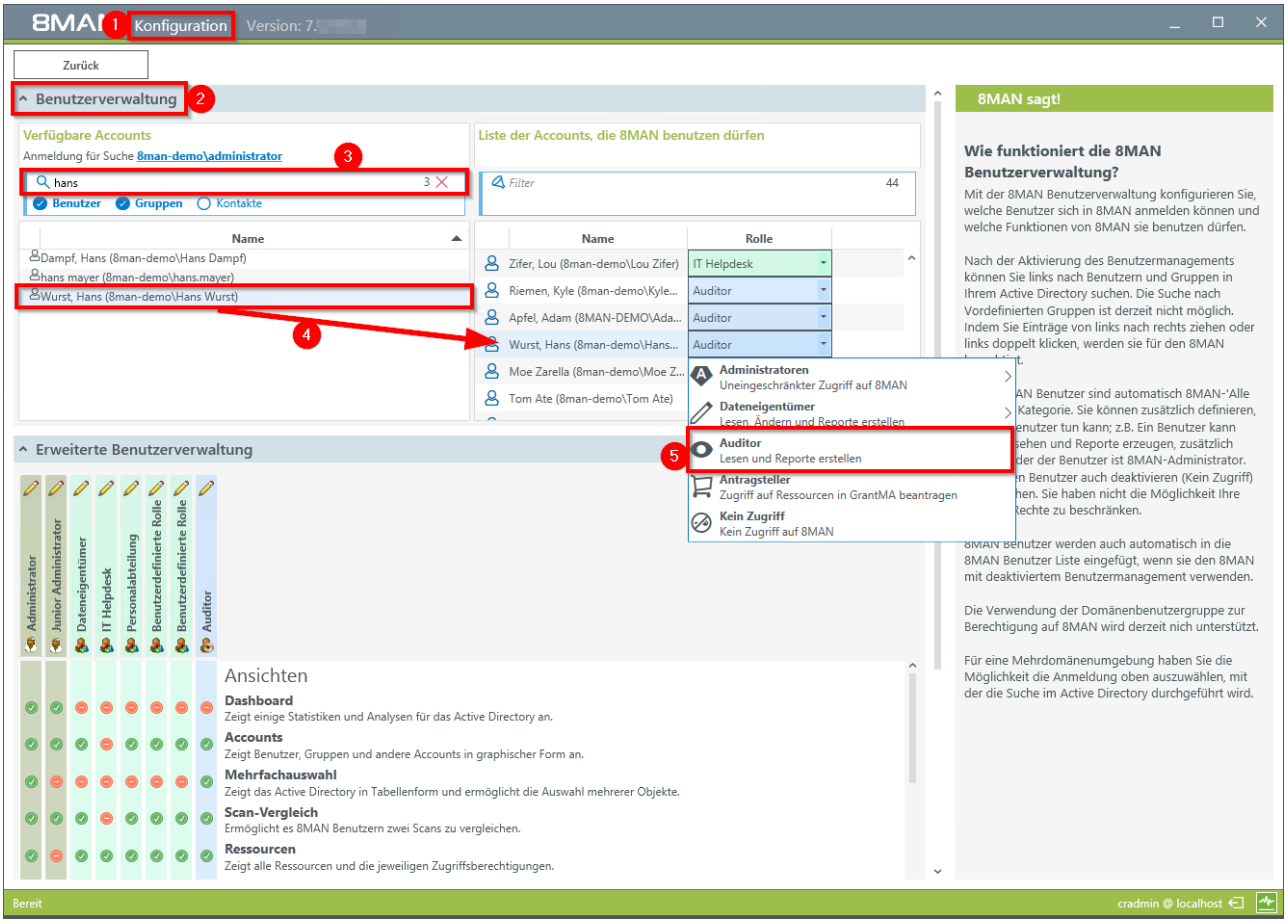
7.1.1.1 Einen einfachen Leseaccount in 8MAN anlegen

Hintergrund / Mehrwert

Involvieren Sie Sicherheitskräfte in das Access Rights Management, indem Sie einen Zugang mit Leserechten vergeben. Damit kann die jeweilige Person auch ihre eigenen Reporte erstellen.

Die Einstellungen nehmen Sie in der 8MAN Konfigurationsoberfläche vor. Sie finden detaillierte Informationen im Handbuch für Installation und Konfiguration, Kapitel 8MAN Benutzer verwalten ff.

Der Prozess in einzelnen Schritten



1. *Starten Sie die 8MAN Konfiguration.*
2. *Wechseln Sie zu "Benutzerverwaltung".*
3. *Nutzen Sie die Suche, um den gewünschten Account zu finden.*
4. *Ziehen Sie den Account per Drag&Drop in die rechte Spalte.*
5. *Wählen Sie in der Spalte Rolle "Auditor".*

Die Einstellungen sind sofort wirksam.

7.1.1.2 Reporte automatisch zusenden lassen

Hintergrund / Mehrwert

Involvieren Sie Sicherheitskräfte in das Access Rights Management, indem Sie pragmatisch die relevanten Reporte zuweisen.
8MAN versendet die Reporte im gewünschten Turnus automatisch. Der Vorgang ist für jeden Report derselbe.

Wir empfehlen eine Auswahl unserer Management Reporte an die Sicherheitsrolle zu senden. Sie sind leicht verständlich und auf das wesentlich reduziert.

Die 8MAN Management Reporte:

Active Directory

Mitarbeiter von Managern
Konto-Details von Nutzern zeigen

Fileserver

Wer hat wo Zugriff?
Wo haben Mitarbeiter eines Managers Zugriff?
Wo haben Benutzer/Gruppen Zugriff?

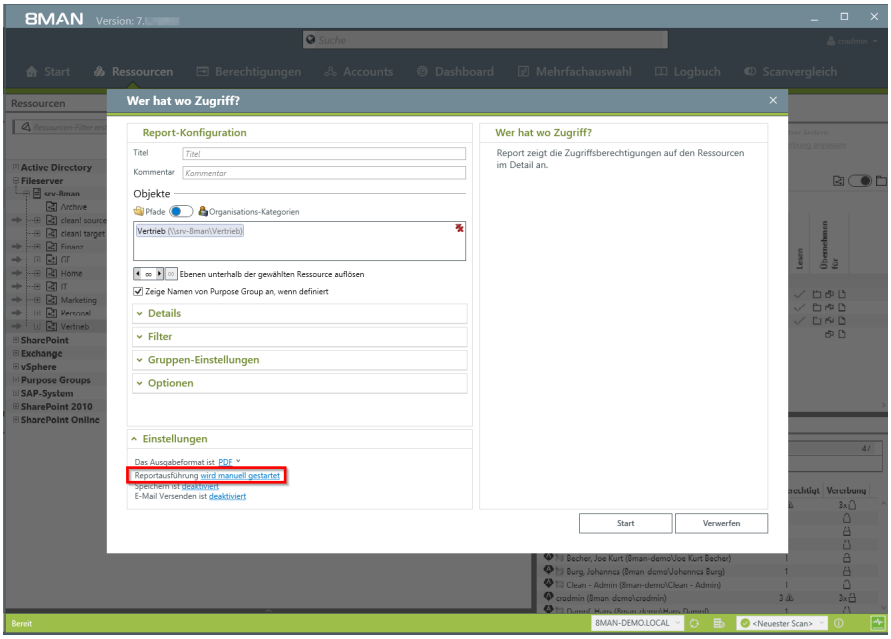
Exchange

Wer hat wo Zugriff?
Postfach Berechtigungen identifizieren

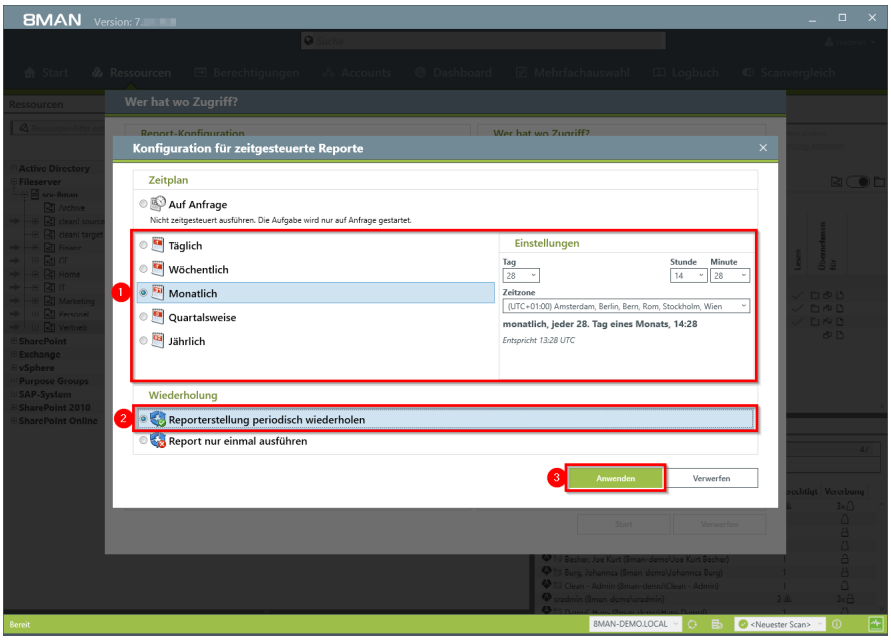
SharePoint

Wer hat wo Zugriff?
Wo haben Benutzer/Gruppen Zugriff

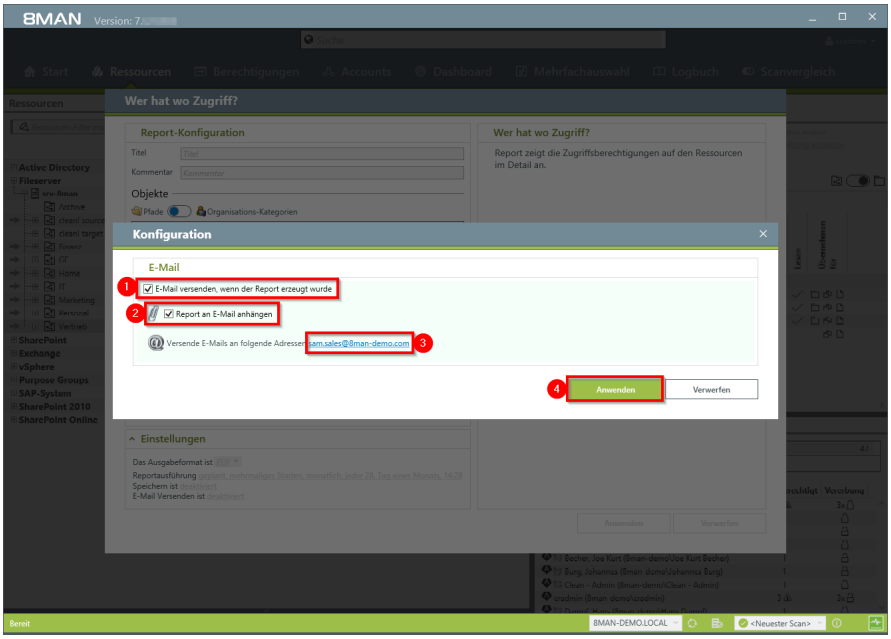
Der Prozess in einzelnen Schritten



Wählen Sie einen beliebigen Report. Klicken Sie im Bereich Einstellungen auf "wird manuell gestartet".



1. *Legen Sie den Zeitplan fest.*
2. *Aktivieren Sie die periodische Wiederholung.*
3. *Klicken Sie auf "Anwenden".*



1. *Aktivieren Sie den E-Mail-Versand.*
2. *Aktivieren Sie die Option "Report an E-Mail anhängen".*
3. *Legen Sie fest, wer die E-Mail erhalten soll. Sie können mehrere Empfänger angeben.*
4. *Klicken Sie auf "Anwenden".*

7.1.2 Die Verwaltung der Verzeichnisrechte an einen Data Owner delegieren

Hintergrund / Mehrwert

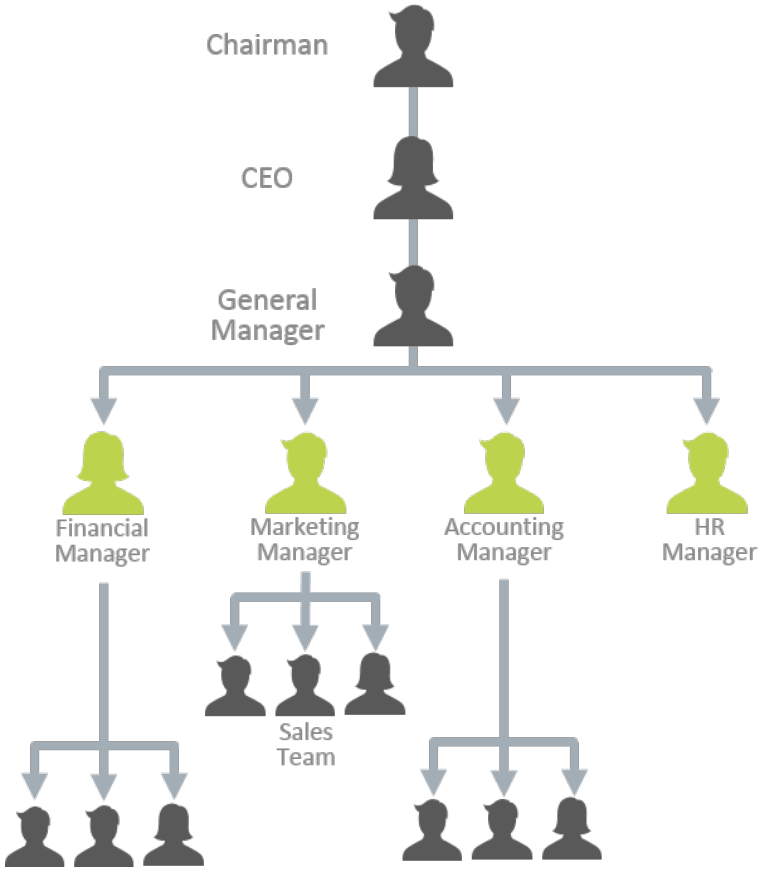
Zentraler Bestandteil von Role und Process Optimization ist die Delegation der Fileserverrechte - Verwaltung an Führungskräfte im Unternehmen.

Als Administrator können Sie in Absprache mit den Leitern der Fachabteilungen sukzessive Data Owner nominieren und Ressourcen zuweisen.

Dies hat den entscheidenden Vorteil, dass die Führungskraft über die Vergabe von Zugriffsrechten entscheidet und gleichzeitig vergibt.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.8 Vergabe von Zugriffsrechten.

Dezentralisieren Sie Sicherheitskompetenz und übertragen die Verzeichnisrechte-Verwaltung an Data Owner



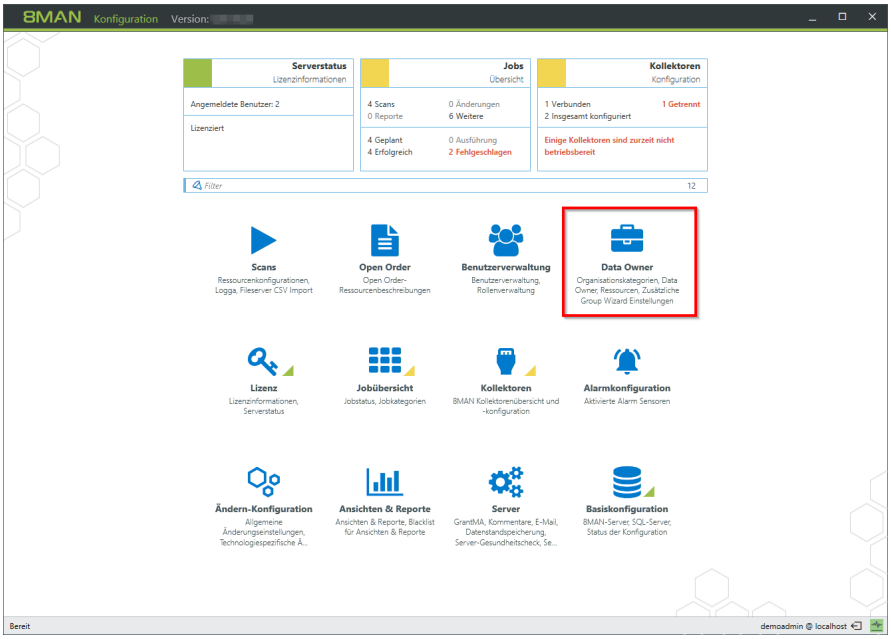
7.1.2.1 Einen Data Owner definieren und ihm Ressourcen zuweisen

Hintergrund / Mehrwert

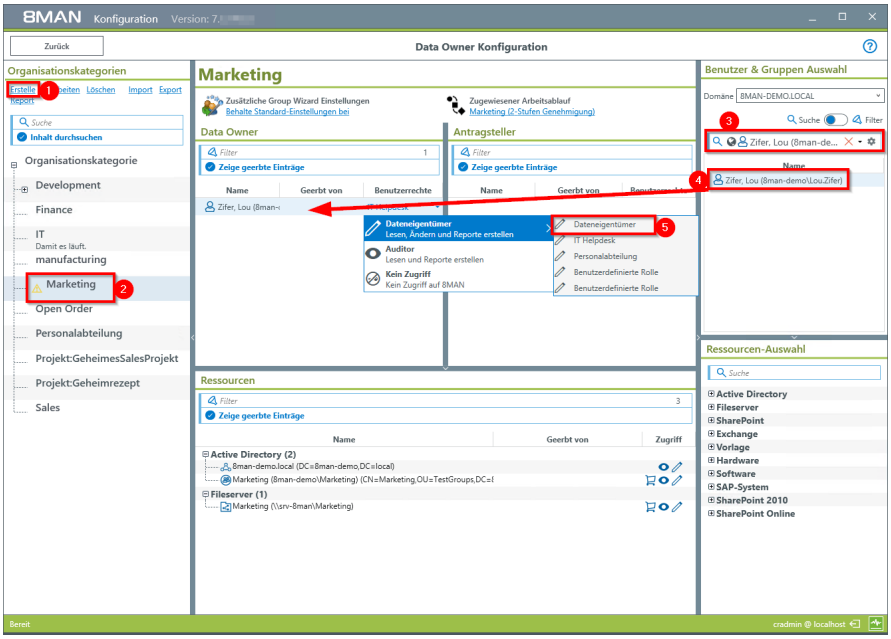
Data Owners bzw. Führungskräfte haben die Verantwortung für den Schutz der digitalen Ressourcen ihrer Abteilung. Mit 8MAN weisen Sie diese individuell zu. Im Folgenden wird eine typische Konfiguration gezeigt.

Die Einstellungen nehmen Sie in der 8MAN Konfigurationsoberfläche vor. Sie finden detaillierte Informationen im Handbuch für Installation und Konfiguration, Kapitel 8MAN Benutzer verwalten ff. und Data Owner ff.

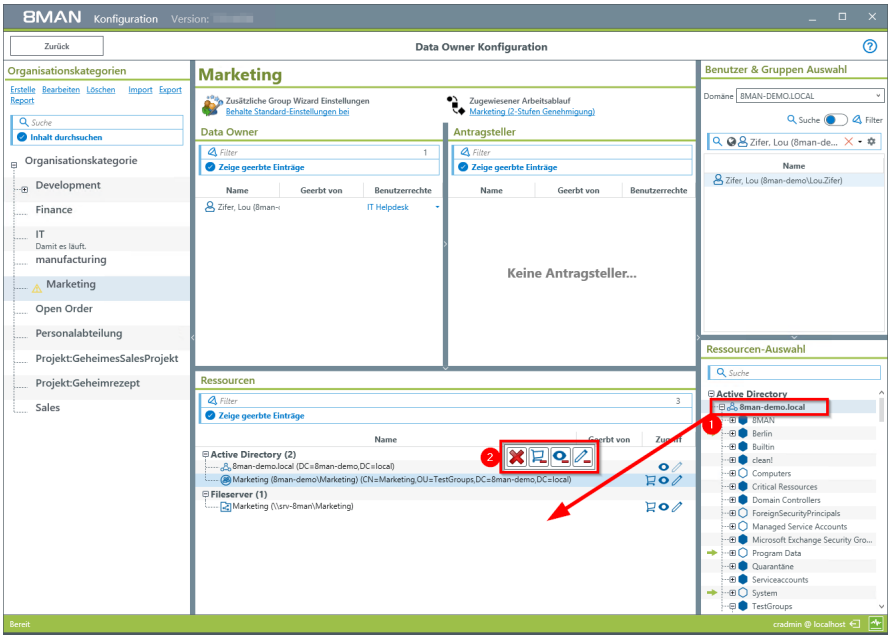
Der Prozess in einzelnen Schritten



Starten Sie die 8MAN Konfiguration und wählen "Data Owner".



1. *Erstellen Sie eine Organisationskategorie, z. B. "Marketing".*
2. *Selektieren Sie die neue Organisationskategorie.*
3. *Nutzen Sie die Suche um den gewünschten Account zu finden.*
4. *Ziehen Sie den Account per Drag&Drop auf die Spalte "Data Owner".*
5. *Wählen Sie in der Spalte "Benutzerrechte" die gewünschte Rolle.*



1. *Ziehen Sie Ressourcen aus der "Ressourcen-Auswahl" per Drag&Drop in den Bereich "Ressourcen". Sie können auch nach Ressourcen suchen.*
2. *Markieren Sie die Ressourcen als "bestellbar, "lesbar" oder "änderbar".*

Beachten Sie, dass Zugriff auf das Active Directory zwingend benötigt wird, wenn der Group Wizard aktiviert ist.

7.1.2.2 Einem Data Owner die Verzeichnisrechte Verwaltung übertragen

Hintergrund / Mehrwert

8MAN erlaubt Ihnen sehr differenzierte Rollen in der Benutzerverwaltung anzulegen. Wir empfehlen mit der Definition eines einfachen Data Owners zu beginnen. Dieser ist in der Lage die Berechtigungen auf Fileserververzeichnisse seiner Mitarbeiter und Abteilung einzusehen (Visor DO Kunden) und zu ändern (Enterprise Kunden).

Der Prozess in einzelnen Schritten

Die Einstellungen nehmen Sie in der 8MAN Konfigurationsoberfläche vor. Sie finden detaillierte Informationen im Handbuch für Installation und Konfiguration, Kapitel 8MAN Benutzer verwalten ff. und Data Owner ff.

7.1.3 User Provisioning Prozesse an den Helpdesk delegieren

Hintergrund / Mehrwert

User Provisioning Prozesse sind leicht delegierbar. Mit 8MAN können Sie sämtliche Aufgaben an den HelpDesk geben. Wir empfehlen mit der Übertragung des einfachen Kontomanagements zu beginnen. Je nach Qualifikationsgrad des Mitarbeiters können Sie die Aufgaben sukzessive erweitern.

Delegierbare Helpdesk-Aufgaben in 8MAN

Active Directory

Benutzerkonto entsperren
Benutzer Kennwort zurücksetzen
Attribute bearbeiten
Benutzerkonto aktivieren/deaktivieren
Benutzerkonto löschen ("Soft Delete")
Einen Nutzer und seine Berechtigungen löschen

Exchange

Postfach anlegen
Postfach-Größe anpassen
Automatische Abwesenheitsnotiz einrichten
Berechtigungen auf Postfächer ändern

7.1.3.1 Den Help Desk in 8MAN definieren und Ressourcen zuweisen

Hintergrund / Mehrwert

8MAN entlastet Administratoren und erlaubt die Delegation von Standardprozessen an den Helpdesk. Dazu ist es notwendig den Helpdesk zu definieren und die Domäne zuzuweisen.

Der Prozess in einzelnen Schritten

Die Einstellungen nehmen Sie in der 8MAN Konfigurationsoberfläche vor. Sie finden detaillierte Informationen im Handbuch für Installation und Konfiguration, Kapitel 8MAN Benutzer verwalten ff. und Data Owner ff.

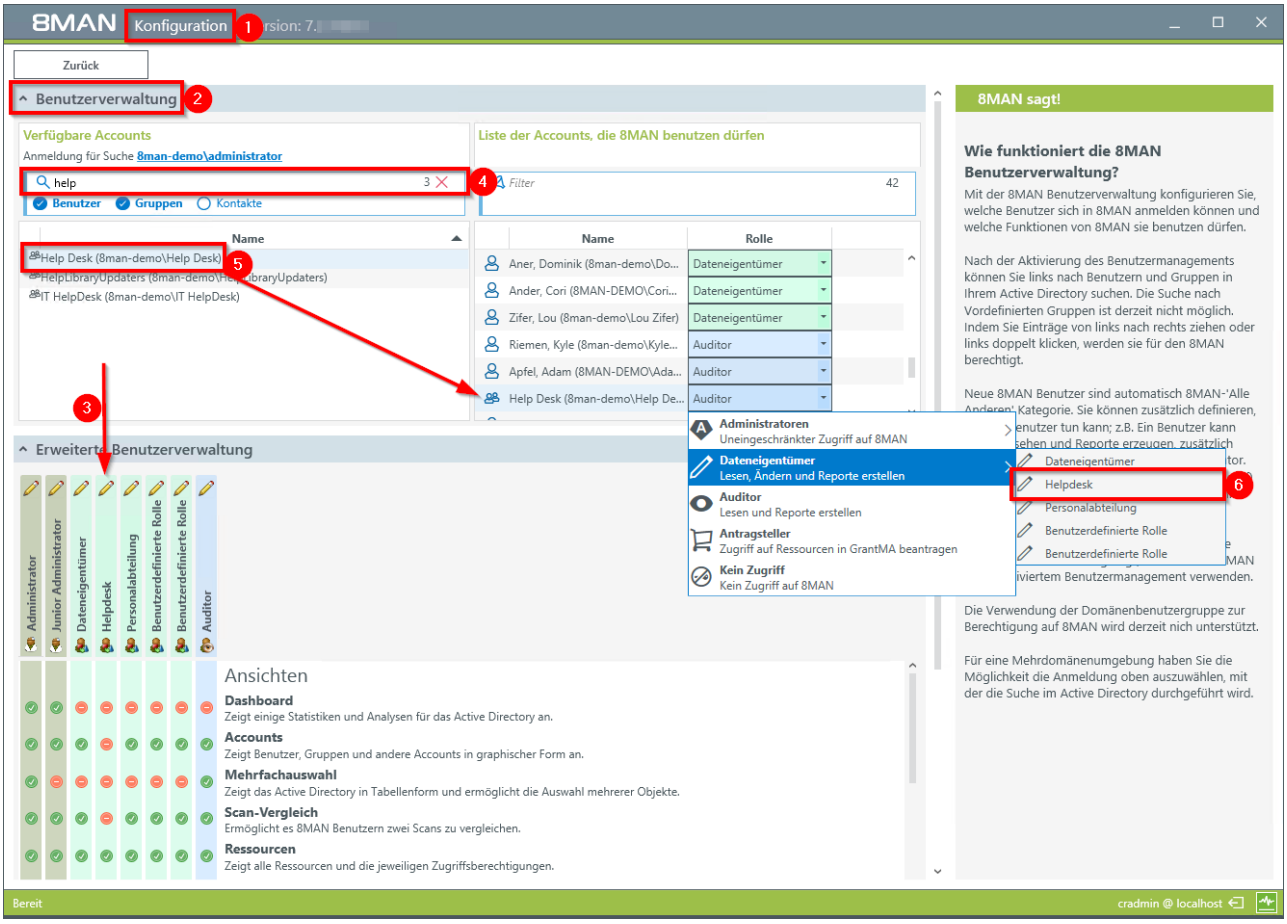
7.1.3.2 Einem Help Desk Mitarbeiter seine Aufgaben zuweisen

Hintergrund / Mehrwert

Sie können das Aufgabenspektrum sehr detailliert für den Helpdesk definieren. Im Folgenden zeigen wir eine typische Funktionszuweisung für einen Helpdesk.

Die Einstellungen nehmen Sie in der 8MAN Konfigurationsoberfläche vor. Sie finden detaillierte Informationen im Handbuch für Installation und Konfiguration, Kapitel 8MAN Benutzer verwalten ff.

Der Prozess in einzelnen Schritten



1. *Starten Sie die 8MAN Konfigurationsoberfläche.*
2. *Wählen Sie den Menüpunkt "Benutzerverwaltung".*
3. *Wählen Sie eine Ändern-Rolle (3. bis 7. Spalte). Ändern Sie den Namen der Rolle nach Klick auf das Stift-Symbol, im Beispiel hier zu "Helpdesk". Aktivieren oder deaktivieren Sie Ansichten und Funktionen für die Rolle "Helpdesk" nach Ihren Anforderungen.*
4. *Nutzen Sie die Suche, um den gewünschten Account zu finden.*
5. *Ziehen Sie den Account per Drag&Drop auf die rechte Spalte.*
6. *Weisen Sie dem Account die Rolle "Helpdesk" zu.*

7.2 Freigabeprozesse erstellen

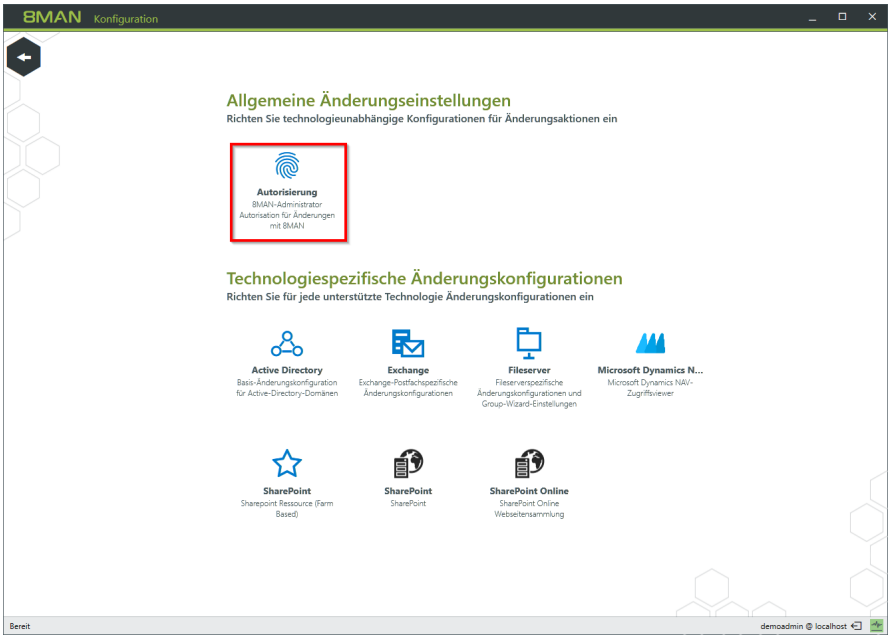
7.2.1 Der einfache Autorisierungsprozess: Als Admin Aktionen freigeben oder ablehnen

Hintergrund / Mehrwert

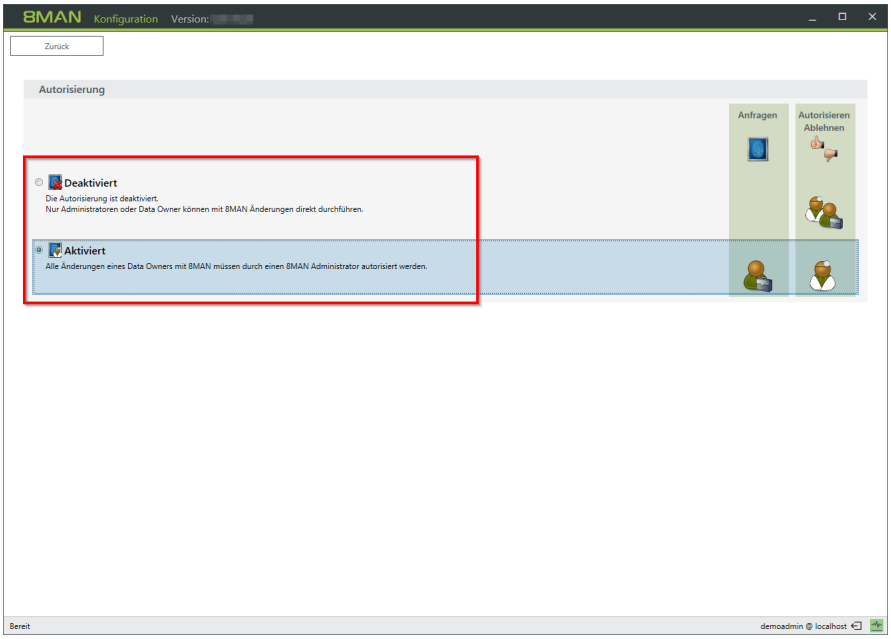
Mit 8MAN können Sie die Prozesse der Data Owners und des Help Desk frei laufen lassen oder kontrollieren. Wir empfehlen insbesondere für den Helpdesk im ersten Schritt als Kontrollinstanz die Prozesse zu beobachten und dezidiert freizugeben.

Im nächsten Schritt, nachdem die Prozesse sich eingeschliffen haben, können Sie den Freigabemodus abstellen.

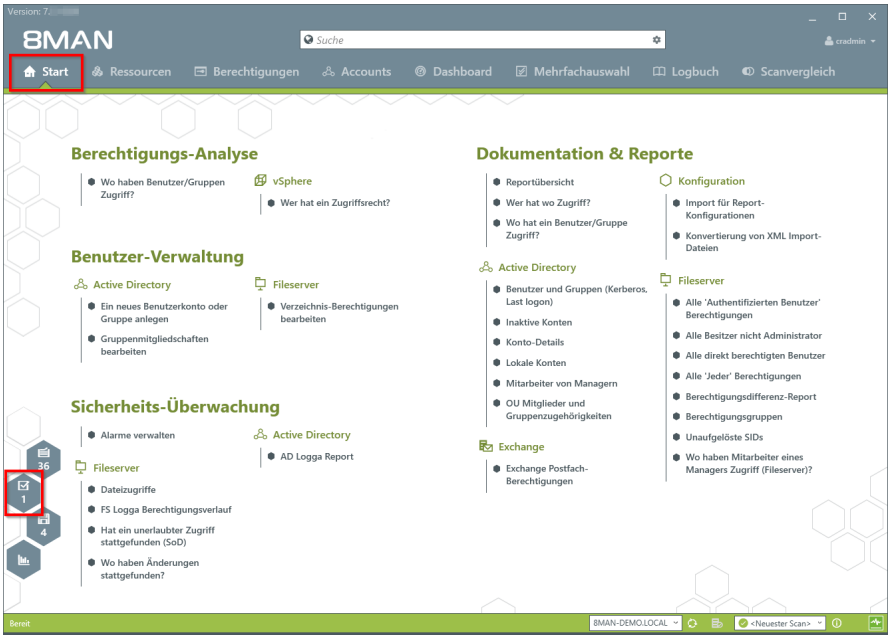
Der Prozess in einzelnen Schritten



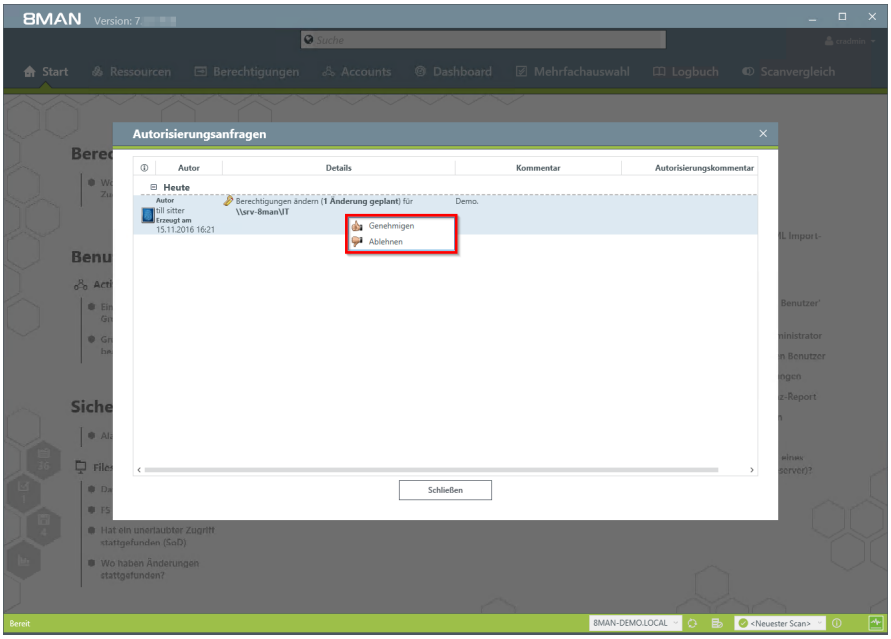
Navigieren Sie in der 8MAN Konfiguration zu "Ändern-Konfiguration" -> "Autorisierung".



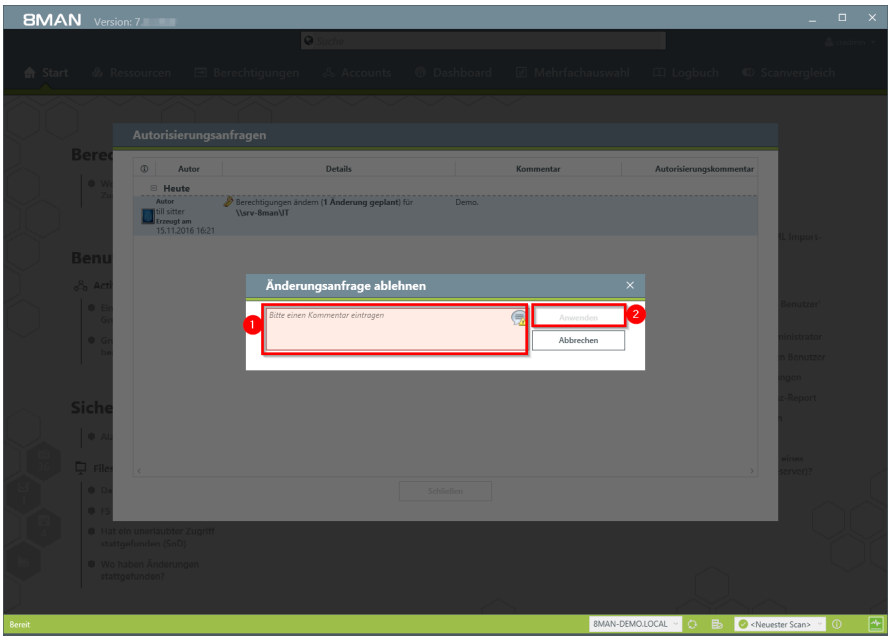
Aktivieren Sie die Administrator-Genehmigung.



Administratoren sehen auf der Startseite offene Genehmigungsanfragen. Klicken Sie auf die Wabe.



Rechtsklicken Sie auf eine Anfrage und treffen Ihre Entscheidung.



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Anwenden".*

7.2.2 +8MATE GrantMA: Komplexe Freigabe-Workflows abbilden

Administratoren verwenden einen guten Teil Ihrer Zeit mit der Vergabe von Zugriffsrechten. Im klassischen Prozess ist die Entscheidung über die Vergabe von Rechten (Vorgesetzter) und die technische Ausführung (Administrator) voneinander getrennt.

Der Administrator weiß nicht, wer welche Rechte haben soll und wird zum reinen Ausführer von Vorgaben.

Es ist effizienter die Bewilligung und tatsächliche Aktivierung von Rechten in einem Schritt zu gestalten. Damit sind nur die Akteure in den Prozess involviert, die wirklich nötig sind.
Der 8MATE GrantMA nutzt einen Workflow, an dem nur der Mitarbeiter und sein Vorgesetzter (Data Owner oder Ressourcenverantwortliche) beteiligt sind:

- Der Mitarbeiter bestellt über ein Webportal seine Berechtigungen.
- Der Data Owner oder Ressourcenverantwortliche entscheidet über die Zugriffsrechte in seiner Abteilung.

Der GrantMA Workflow hat folgende Vorteile:

- Der Administrator ist nicht mehr Teil des Prozesses und kann sich auf seine Kernaufgaben konzentrieren
- Der Data Owner, der am besten die Informationsstruktur der Abteilung kennt, entscheidet über die Freigabe von Daten und vergibt die Rechte in einem Schritt
- Durchgeführte Änderungen werden revisionssicher im 8MAN Logbuch protokolliert

Werden komplexere Workflows mit mehreren Entscheidern für die Vergabe von Zugriffsrechten benötigt, können Sie diese ebenfalls schnell abbilden.

7.2.2.1 Individuelle Freigabeworkflows definieren

Hintergrund / Mehrwert

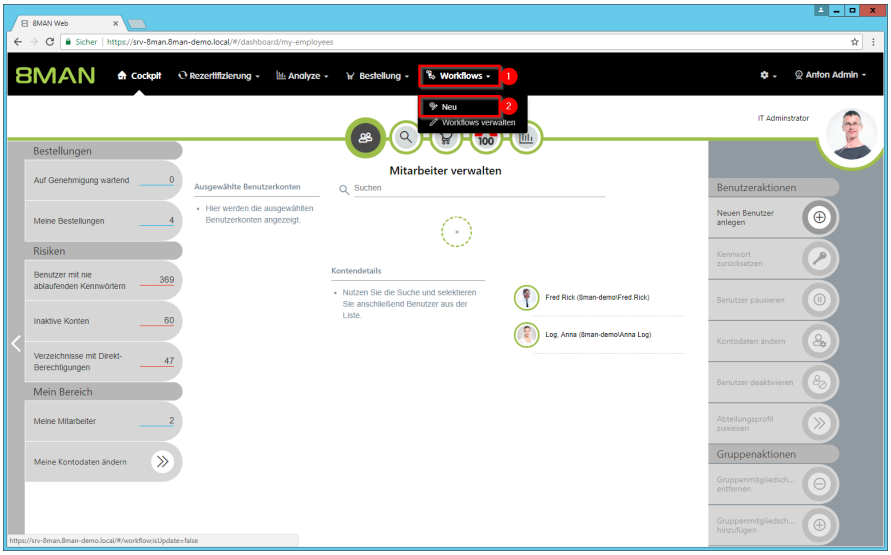
Mit dem 8MATE GrantMA erstellen Sie für jede Organisationskategorie individuelle Genehmigungsworkflows. Je nach Anforderung lassen sich unbegrenzt viele Stufen konfigurieren. Der letzte Genehmiger im Prozess führt gleichzeitig die Bestellung aus.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.8 Vergabe von Zugriffsrechten.

Weiterführende Services

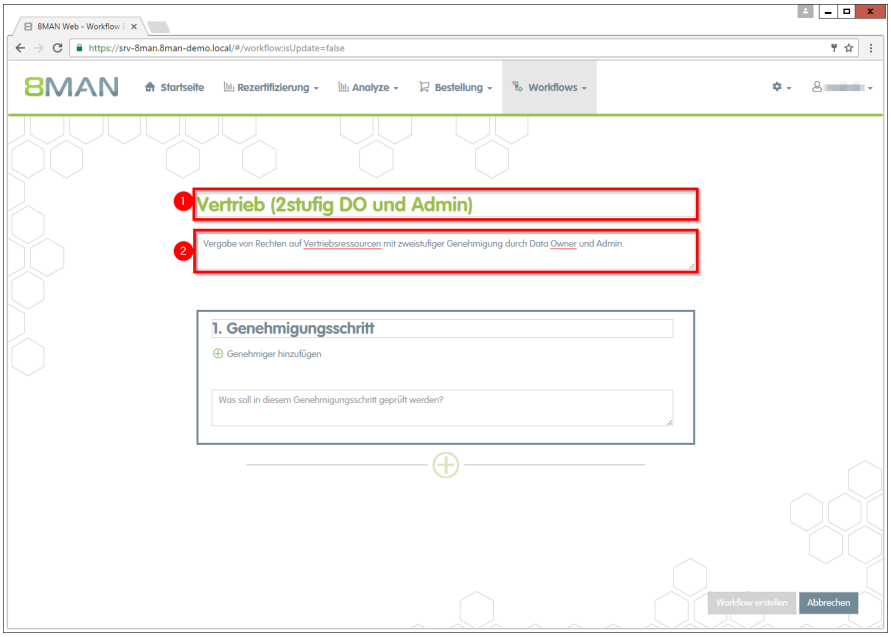
Den individuellen Freigabeworkflow den Ressourcen zuweisen

Der Prozess in einzelnen Schritten

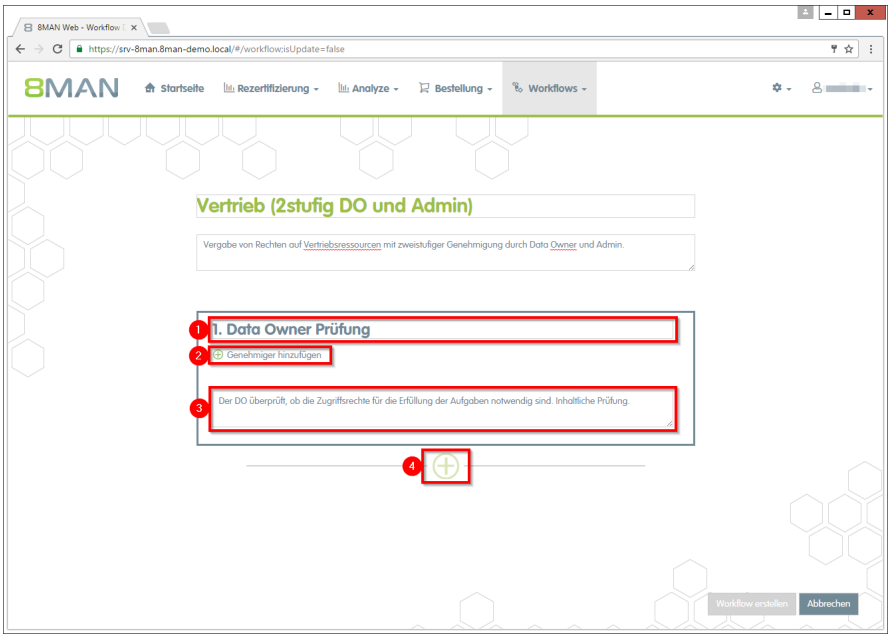


Loggen Sie sich als 8MAN Administrator auf dem GrantMA-Portal ein.

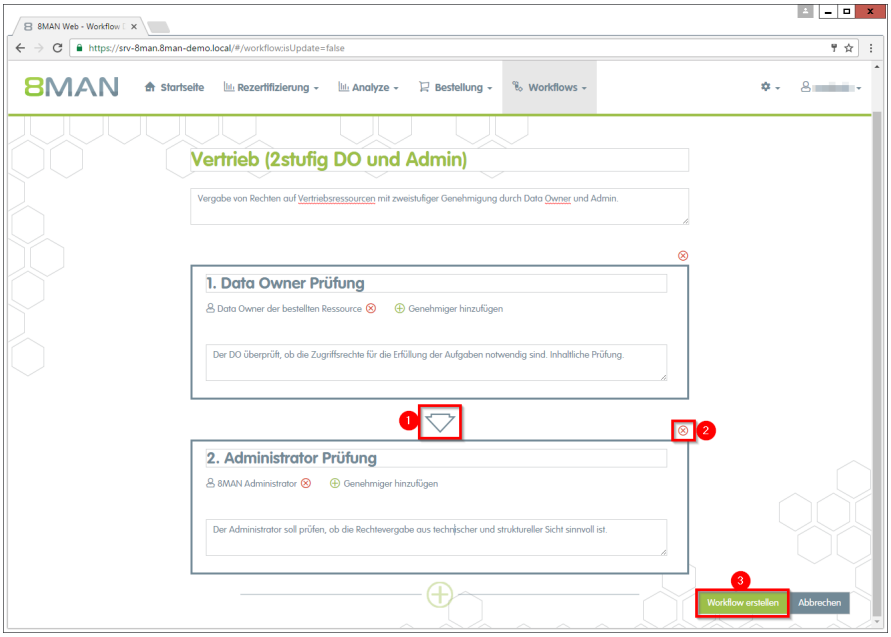
1. *Wählen Sie "Workflows".*
2. *Klicken Sie auf "Neu".*



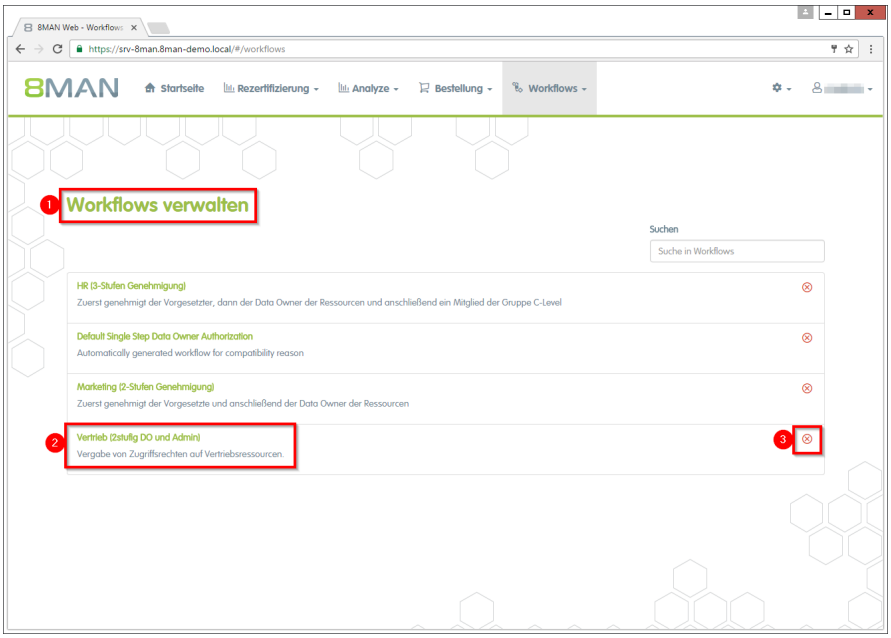
1. *Geben Sie Ihrem Workflow einen aussagekräftigen Namen.*
2. *Beschreiben Sie kurz und prägnant, wozu der Workflow genau dient.*



1. *Geben Sie dem Genehmigungsschritt einen Namen.*
2. *Fügen Sie einen oder mehrere Genehmiger hinzu.* **Hinterlegen sie pro Schritt mehr als eine Person, um im Urlaubs- oder Krankheitsfall die Prozesseffizienz aufrecht zu erhalten.**
3. *Beschreiben Sie den Genehmigungsschritt.*
4. *Fügen Sie einen weiteren Genehmigungsschritt hinzu.*



1. *Fügen Sie einen Zwischenschritt hinzu.*
2. *Entfernen Sie einen Genehmigungsschritt.*
3. *Erstellen Sie den Workflow.*



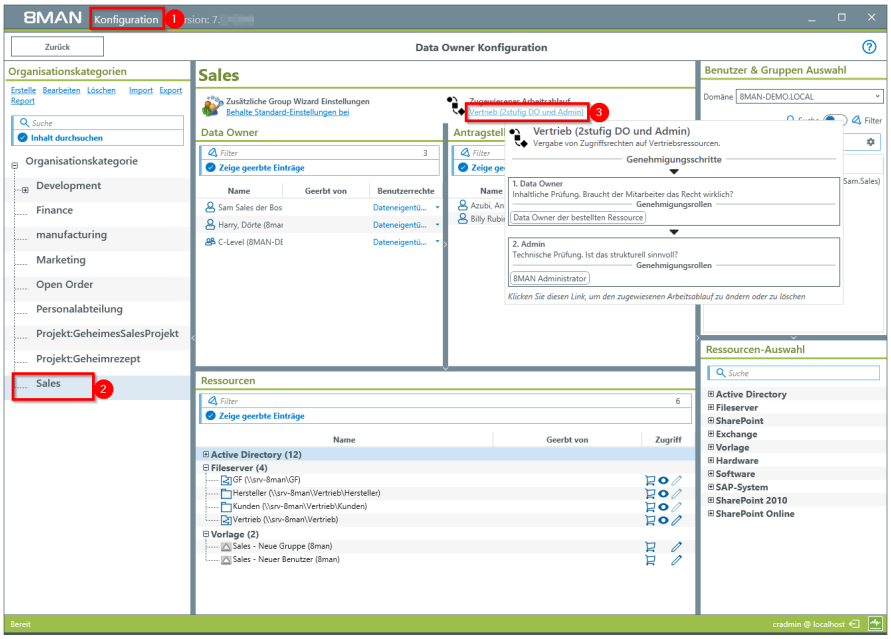
1. *Sie haben den neuen Workflow erstellt und 8MAN wechselt in die Ansicht "Workflows verwalten".*
2. *Klicken Sie auf einen Workflow, um ihn zu ändern.*
3. *Löschen Sie einen Workflow.*

7.2.2.2 Den individuellen Freigabeworkflow den Ressourcen zuweisen

Hintergrund / Mehrwert

Verknüpfen Sie die bestellbaren Ressourcen mit Ihren individuellen Workflows.

Der Prozess in einzelnen Schritten



1. *Starten Sie die 8MAN Konfigurationsoberfläche und wählen Sie "Data Owner".*
2. *Selektieren Sie eine Organisationskategorie.*
3. *Weisen Sie einen Workflow zu.*

7.2.2.3 Ressourcenverantwortliche im Webclient definieren

Hintergrund / Mehrwert

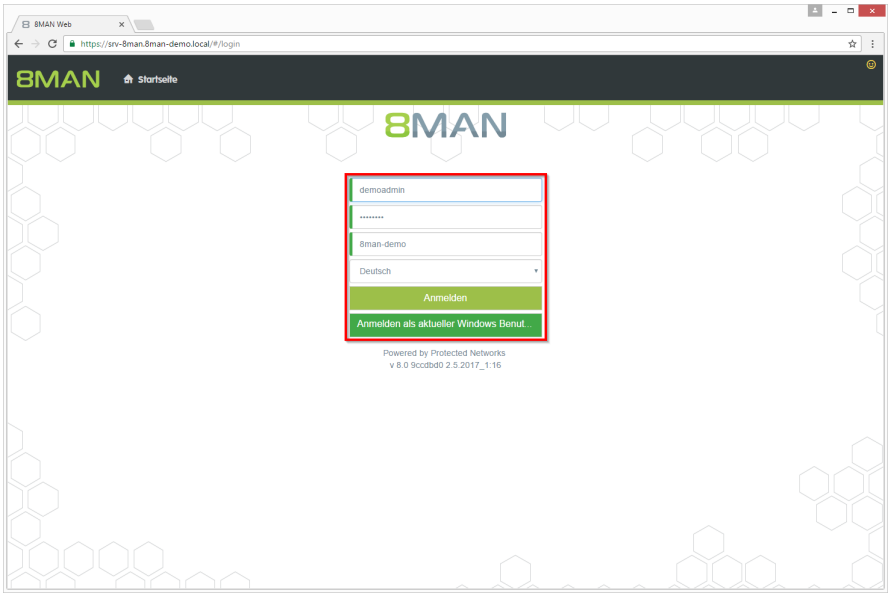
Mit der Version 8.0 entwickeln wir den 8MATE GrantMA weiter und führen eine neue Genehmiger-Rolle ein: "Ressourcenverantwortlicher". Die Zuweisung dieser Rolle zu den Ressourcen erfolgt vollständig im Webclient. Auf Kundenwunsch erfolgt die Zuweisung direkt zwischen Ressource und Verantwortlichen, ohne die in der bisherigen Data Owner Konfiguration erforderliche Bildung von Organisationskategorien.

Die Funktionalität ist standardmäßig deaktiviert. Zum Aktivieren wenden Sie sich an unseren Support oder lesen den Support Knowledgebase Artikel (Support Login erforderlich).

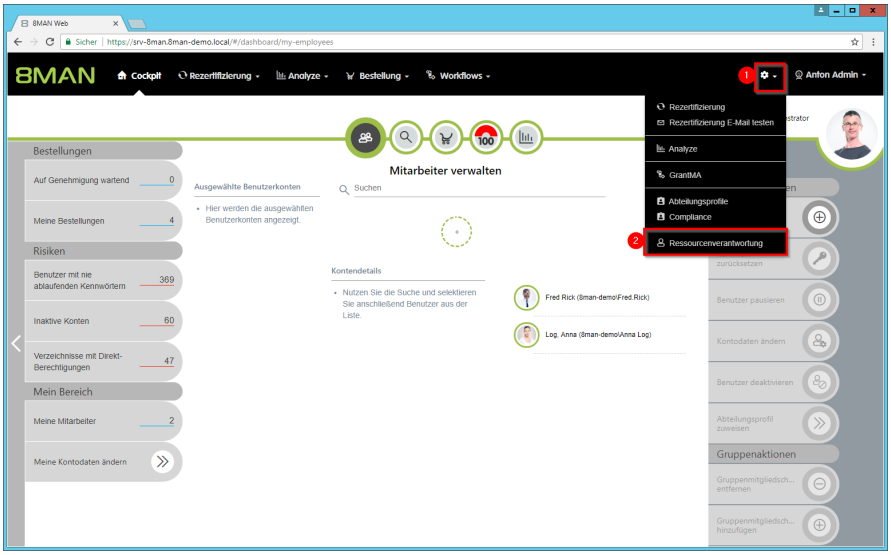
Weiterführende Services

Verwenden Sie den Ressourcenverantwortlichen, in dem Sie ihn als Genehmiger in individuellen Workflows definieren.

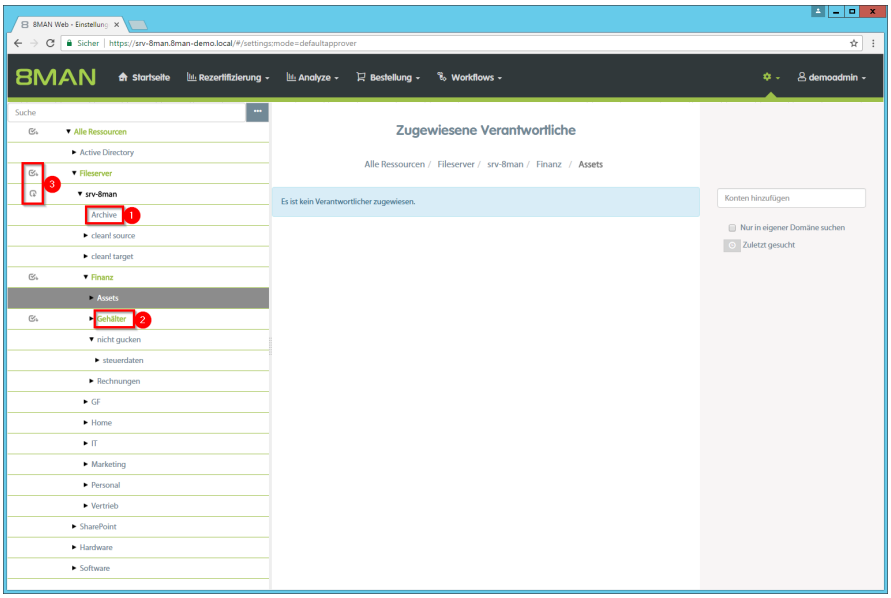
Der Prozess in einzelnen Schritten



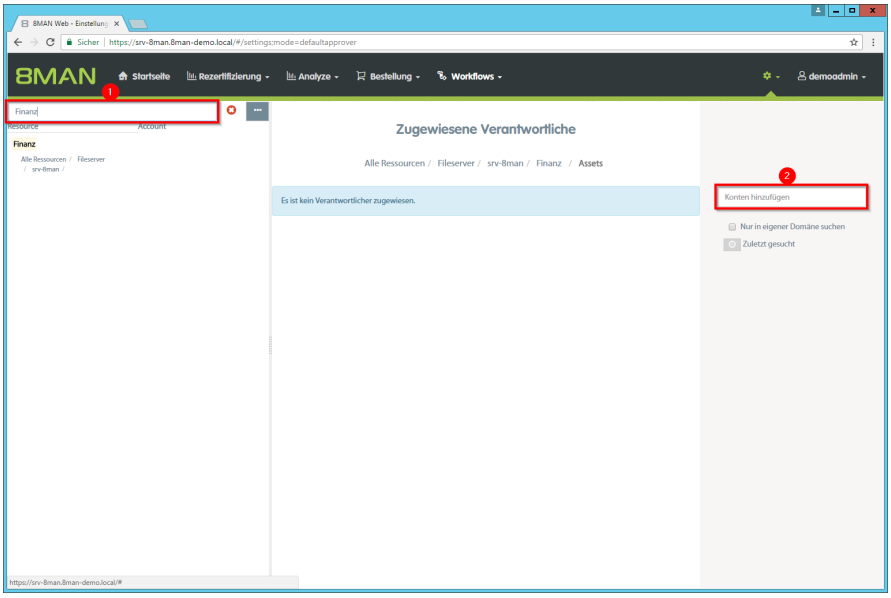
Loggen Sie sich als Administrator in die 8MAN Weboberfläche ein.



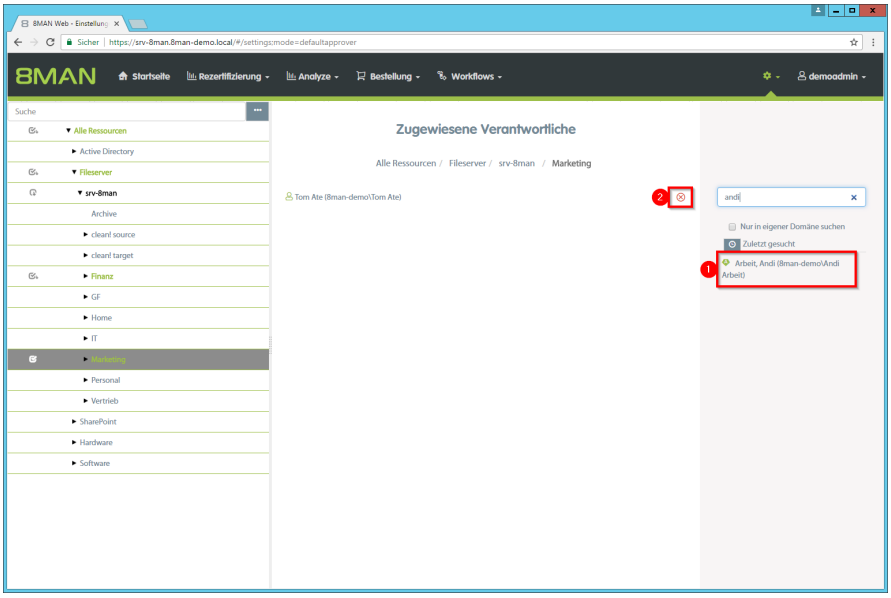
1. *Klicken Sie auf das Zahnrad.*
2. *Wählen Sie "Ressourcenverantwortung ".*



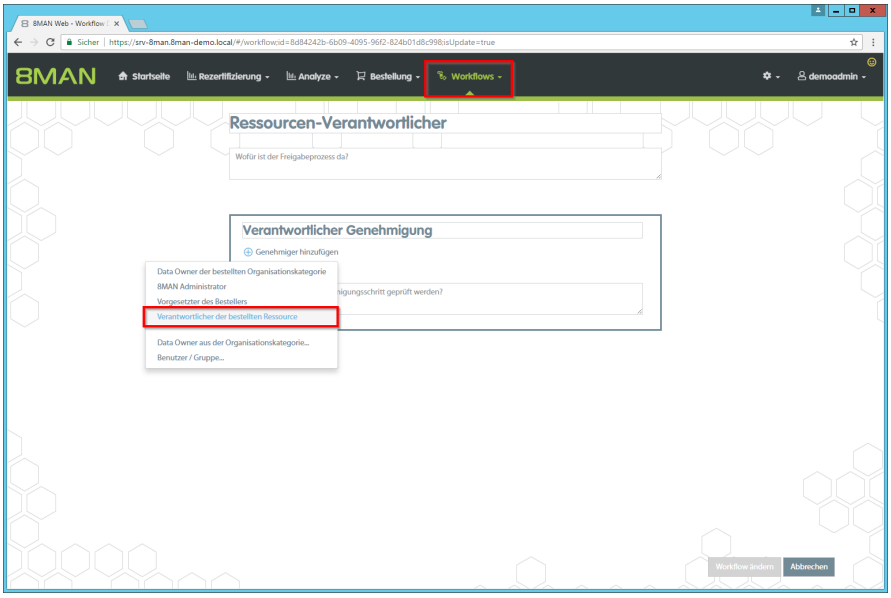
1. *Graue Schrift bedeutet, dass für diese Ressource kein Verantwortlicher zugewiesen ist.*
2. *Grüne Schrift bedeutet, dass für diese Ressource ein Verantwortlicher zugewiesen wurde.*
3. *Die Symbole zeigen an, ob in den untergeordneten Ressourcen bereits Zuweisungen existieren. Fahren Sie mit dem Mauszeiger über ein Symbol, um eine Erklärung zu erhalten.*



1. *Nutzen Sie die Suche, um eine Ressource oder einen zugewiesenen Ressourcenverantwortlichen zu finden.*
2. *Benutzen Sie das Suchfeld, um ein Konto zu finden.*



1. *Klicken Sie auf ein gefundenes Konto, um es zuzuweisen.*
2. *Klicken Sie auf das Symbol, um eine Zuordnung zu entfernen.*



Verwenden Sie den Ressourcenverantwortlichen, in dem Sie ihn als Genehmiger in individuellen Workflows definieren.

7.3 Data Owner: Bestehende Zugriffsrechte rezertifizieren

Hintergrund / Mehrwert

Sicherheitsregularien fordern die Einhaltung des Least-Privilege-Prinzips. Dazu prüfen Sie als Data Owner in regelmäßigen Abständen die Berechtigungssituation auf Ihre Ressourcen. Im Rahmen der 8MAN Rezertifizierung erhalten Sie eine E-Mail und gelangen in eine einfache Ansicht, in der alle Ressourcen und Zugriffsberechtigte aufgelistet sind. Sie müssen dann für jede Ressource entscheiden, ob das Zugriffsrecht belassen oder entfernt werden soll.

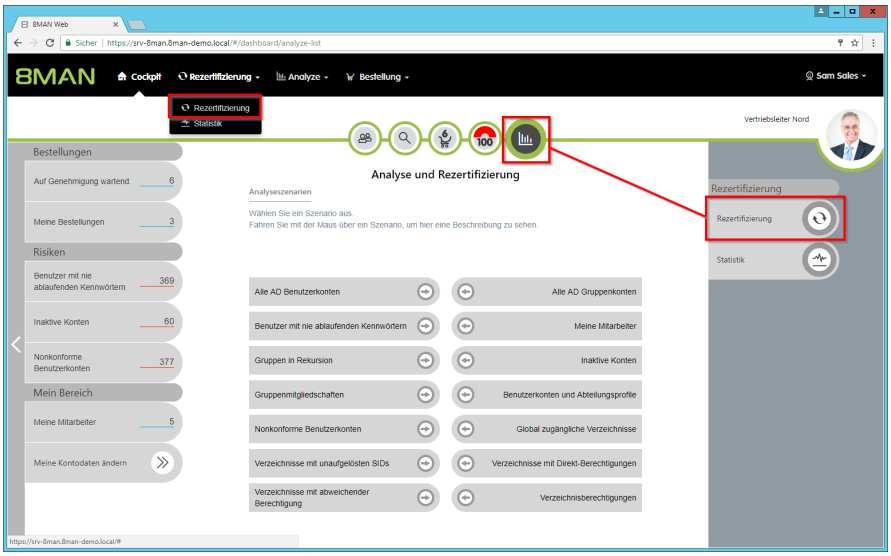
Ihre Änderungswünsche werden nach Abschluss an den zuständigen Administrator übermittelt.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 2.8 Vergabe von Zugriffsrechten.

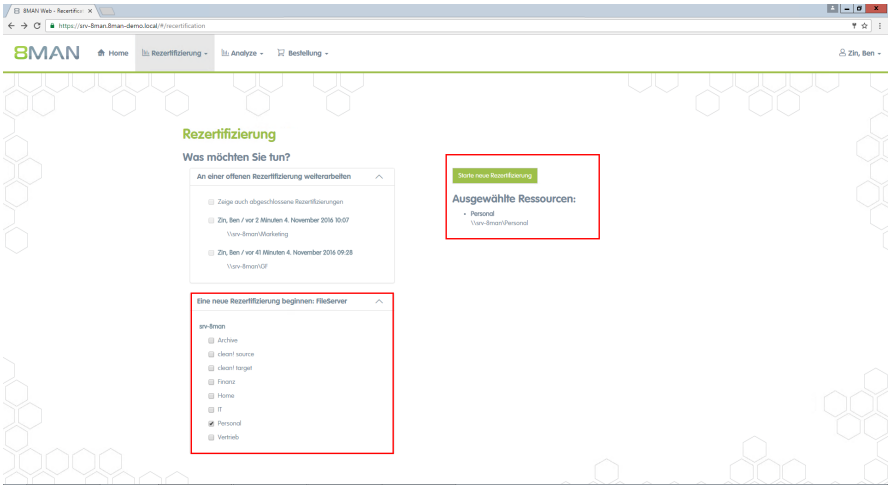
Weiterführende Services

Verzeichnisberechtigungen ändern
Verzeichnisse für die Rezertifizierung konfigurieren (Administrator)

Der Prozess in einzelnen Schritten



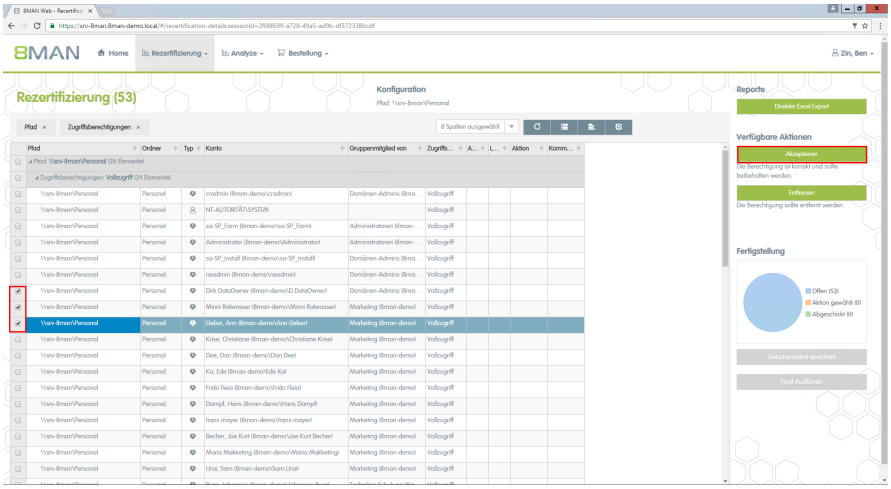
Klicken Sie im Webclient auf „Rezertifizierung“.



Sie erhalten eine Übersicht mit all Ihren Ressourcen.

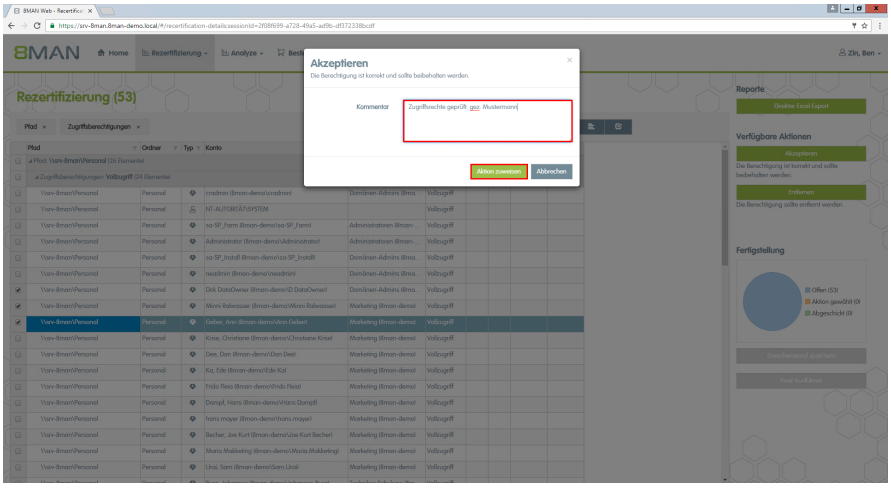
Wählen Sie „Eine neue Rezertifizierung beginnen“. Klicken Sie auf ein oder mehrere Verzeichnisse.

Die ausgewählten Ressource sind auf der rechten Seite gelistet. Klicken Sie auf „Starte neue Rerzertifizierung“.

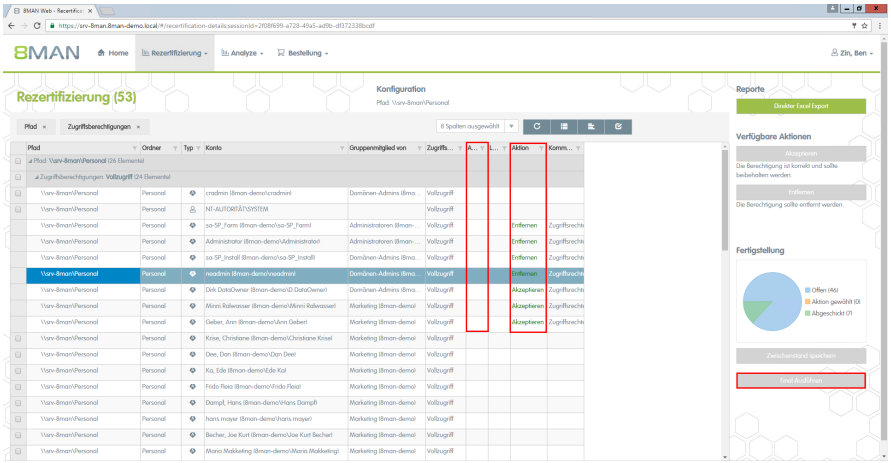


Sie können bestehende Berechtigungen akzeptieren oder entfernen lassen. Aktivieren Sie erst alle Nutzer, die ihren Zugriff behalten sollen. Klicken Sie auf „Akzeptieren“.

Unterordner werden nur angezeigt, wenn diese über abweichende Berechtigungen verfügen.



Kommentieren Sie Ihre Entscheidung. Sie wird revisionssicher im System dokumentiert.



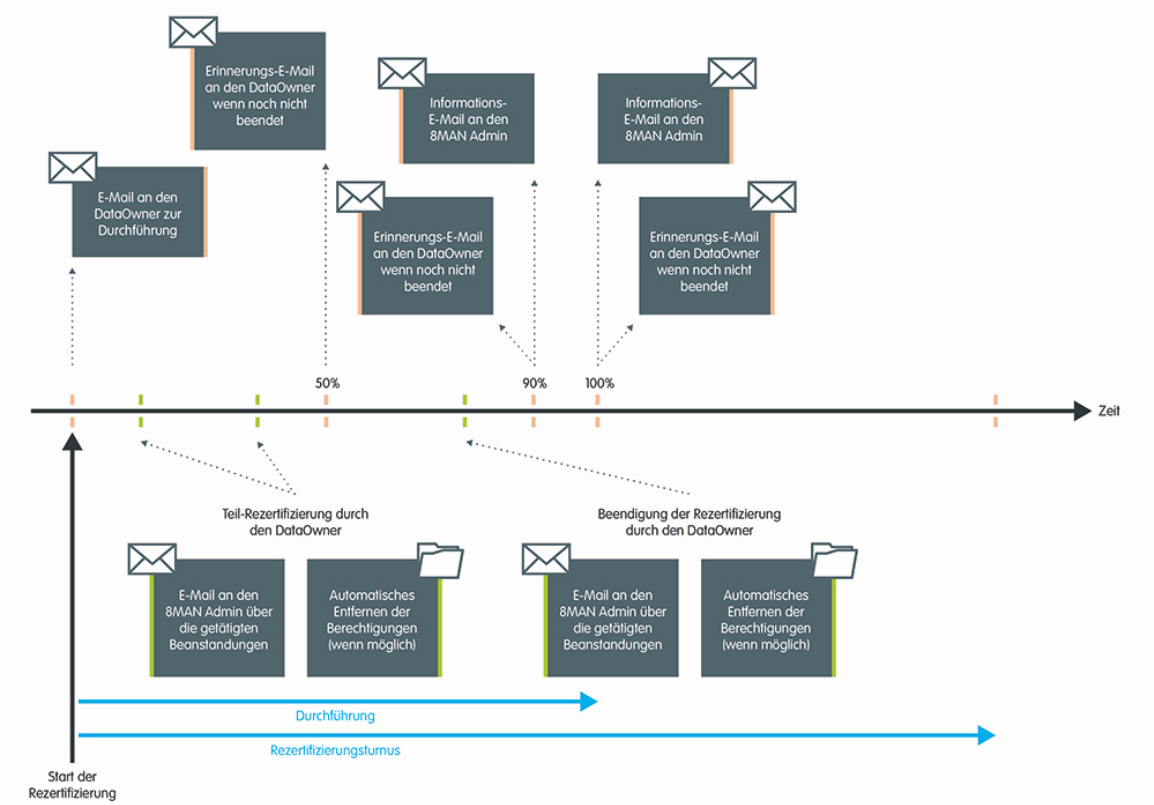
Verfahren Sie genauso mit den Zugriffsrechten, die entzogen werden sollen.

Ihre Entscheidung sehen Sie in der Spalte Aktion. Klicken Sie auf „Final Ausführen“. Der Administrator erhält nach Finalisierung eine Liste für die Umsetzung.

Temporär berechtige Nutzerkonten (siehe eingerückte Spalte in der Abbildung), die gleichzeitig über eine weitere, unbegrenzte Berechtigung auf ein Verzeichnis verfügen, werden unwirksam und entsprechend nicht mehr in der Spalte Ablaufdatum angezeigt.

Wenn Sie "Final Ausführen" klicken, bekommt Ihr Administrator fast jedes Mal eine E-Mail mit den Änderungswünschen. Deshalb empfehlen wir den Rezertifizierungsprozess in einem Rutsch durchzuführen.

7.3.1 E-Mail Aufforderungen zur Rezertfizierung



8MAN sendet Ihnen im Rezertifizierungszeitraum automatische Reminder für die Durchführung der Rezertifizierung.

Wenn Sie die Rezertifizierung nicht vor Ende der Periode beenden, stoppt 8MAN den Prozess und Sie und der Administrator erhalten eine Meldung über fehlende Umsetzung.

7.4 +8MATE GrantMA Workflows für Mitarbeiter

Mitarbeiter können über das 8MATE GrantMA Self-Service Portal bei verschiedenen Rollen im Unternehmen Ressourcen bestellen.
Wir haben zur Veranschaulichung eine Reihe typischer Prozesse für Sie veranschaulicht.

Die Services im Überblick:

Fileserver Rechte beim Data Owner bestellen
Einen Bestellprozess über den Einkauf initiieren (Open Order)
Als HR Mitarbeiter beim Help Desk ein Nutzerkonto erstellen lassen

7.4.1 Meine Bestellungen verwalten (Cockpit)

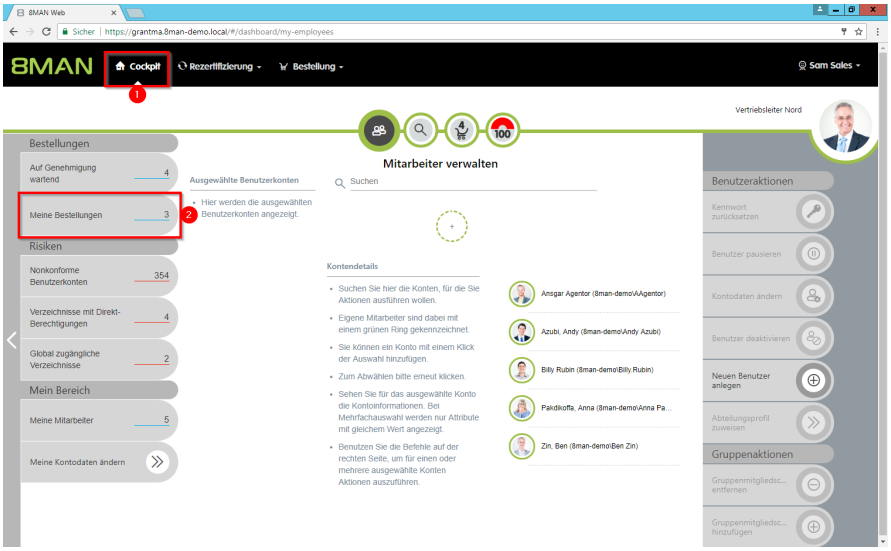
Hintergrund / Mehrwert

Behalten Sie den Überblick über Ihre Bestellungen. Stornieren Sie Bestellungen oder senden Sie erneute Benachrichtigungen an den Genehmiger.

Weiterführende Services

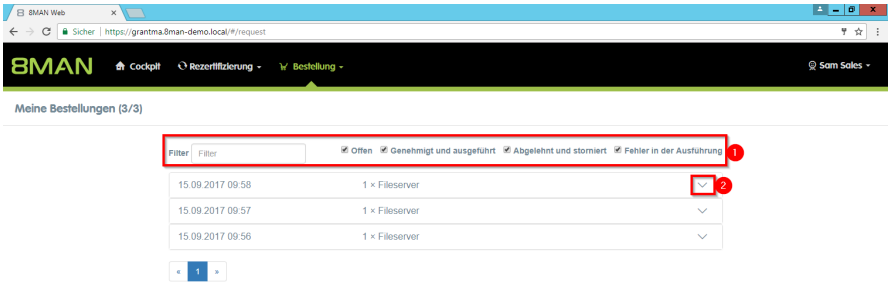
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

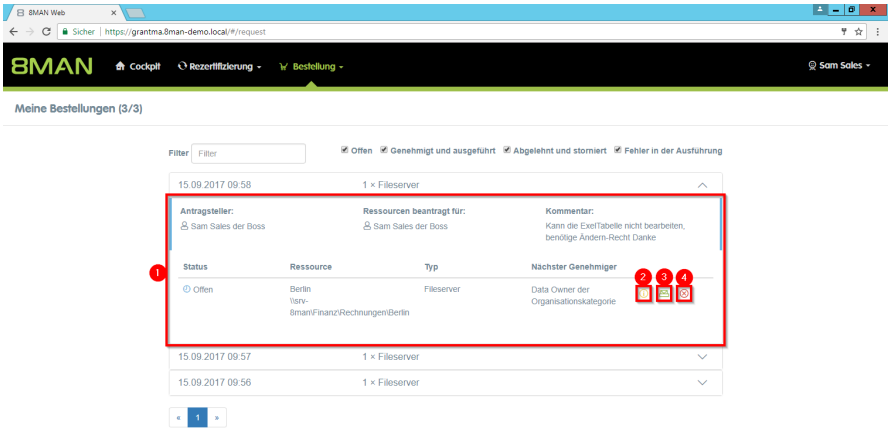


1. *Wählen Sie Cockpit.*
2. *Klicken Sie auf meine Bestellungen. In dem Beispiel hat Sam Sales "3" Bestellungen.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Filtern Sie Ihre Bestellungen, um bei vielen Einträgen schnell die gewünschte Bestellung zu finden.*
2. *Klappen Sie die gewünschte Bestellung auf.*



1. *8MAN zeigt Ihnen Details zur Bestellung.*
2. *Lassen Sie sich weitere Einzelheiten zur Bestellung anzeigen.*
3. *Versenden Sie erneut eine Benachrichtigungs-E-Mail an den Genehmiger.*
4. *Stornieren Sie Ihre Bestellung.*

7.4.2 Fileserverrechte bestellen

Hintergrund / Mehrwert

Im 8MATE GrantMA Self-Service-Portal bestellen Mitarbeiter Fileserver-Rechte bei Data Owners oder Ressourcenverantwortlichen. Damit wird Access Rights Management zu einem kurzen, kontrollierbaren und dokumentierten Prozess.

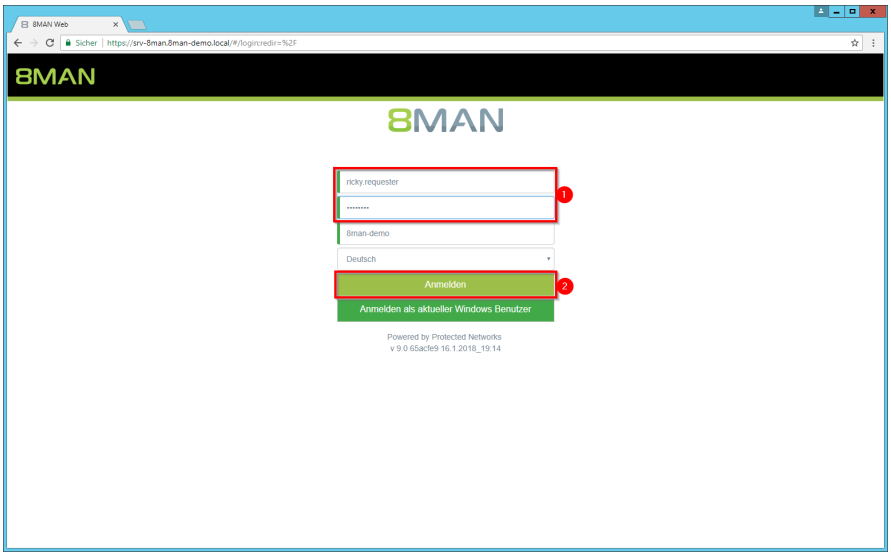
Je nach Sicherheitslevel können Sie unterschiedlich komplexe Freigabeprozesse definieren und die relevanten Entscheider involvieren.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen.

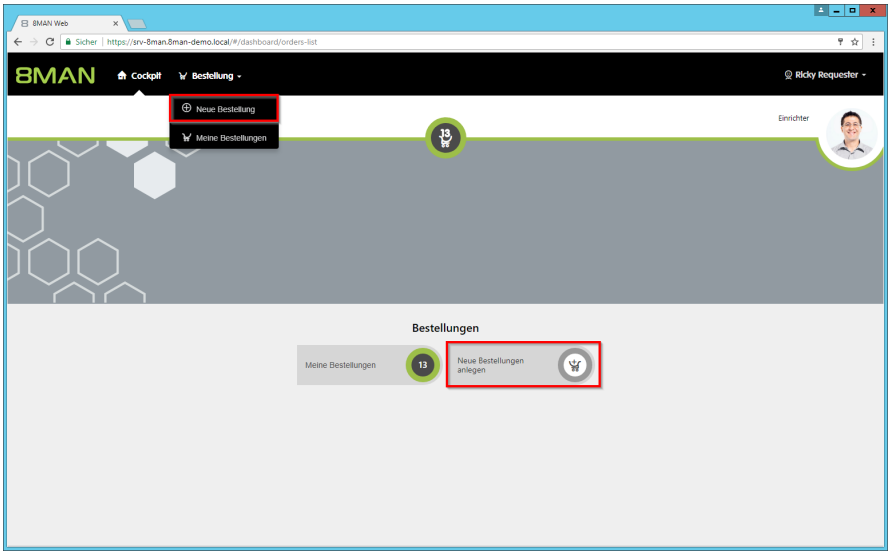
Weiterführende Services

Individuelle Freigabeworkflows definieren (Administrator)

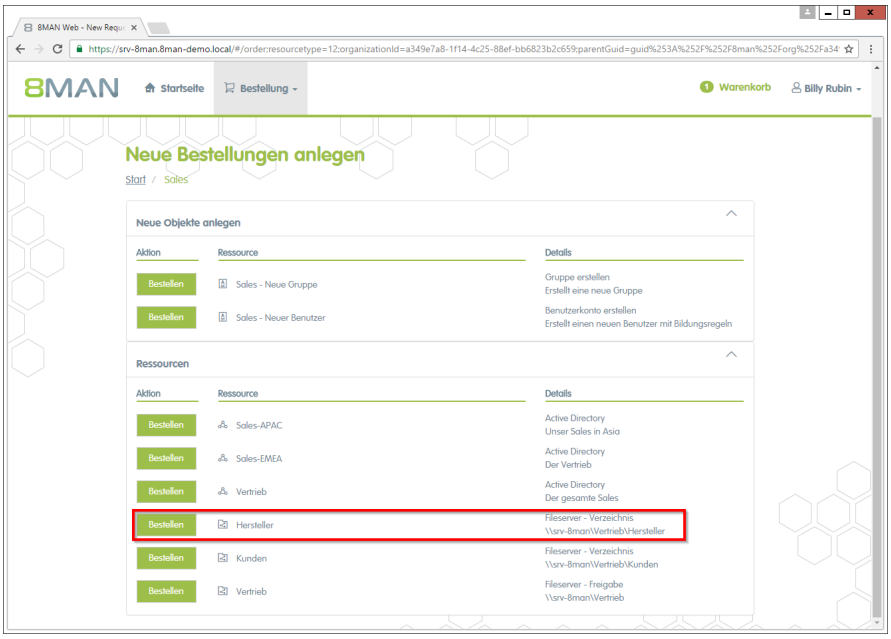
Der Prozess in einzelnen Schritten



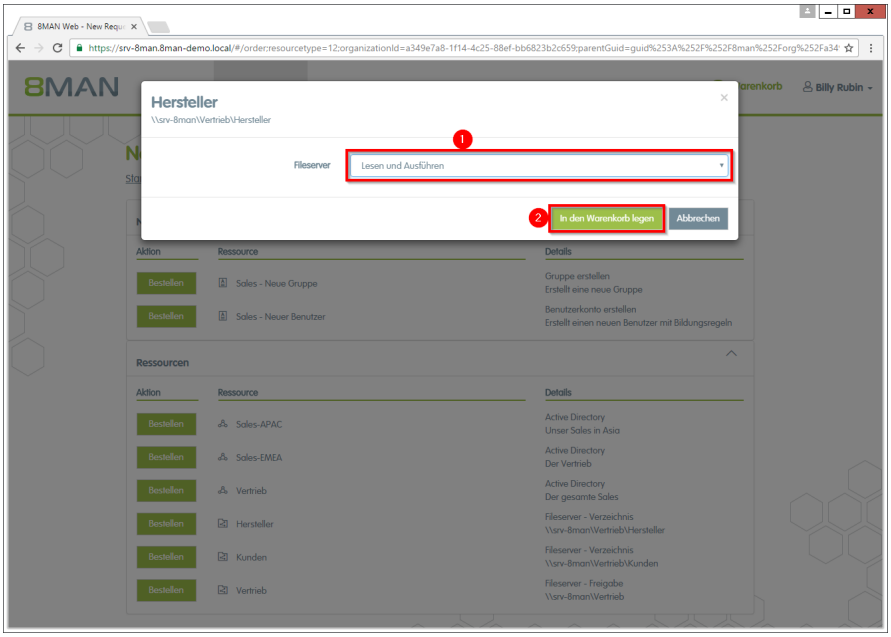
1. *Geben Sie Benutzername und Kennwort ein.*
2. *Klicken Sie auf "Anmelden".*



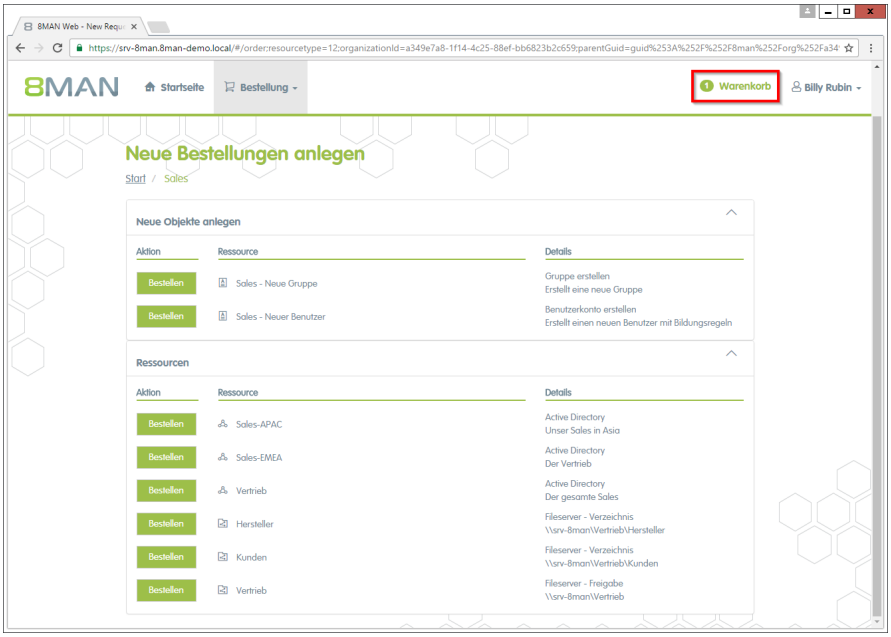
Klicken Sie auf "Neue Bestellung".



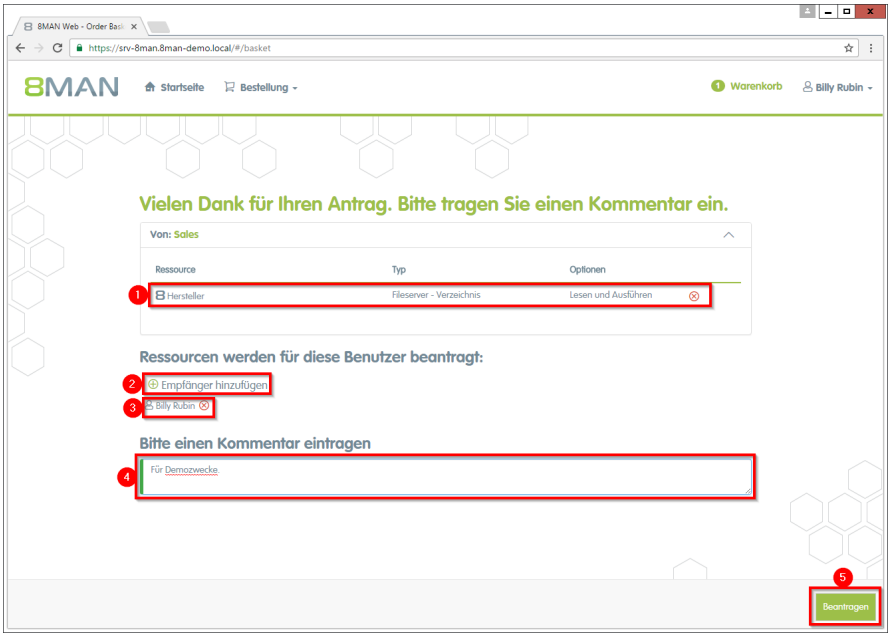
8MAN zeigt Ihnen als Antragsteller genau die Ressourcen, die für Sie bestellbar sind. Wählen Sie die gewünschte Ressource und klicken auf "Bestellen".



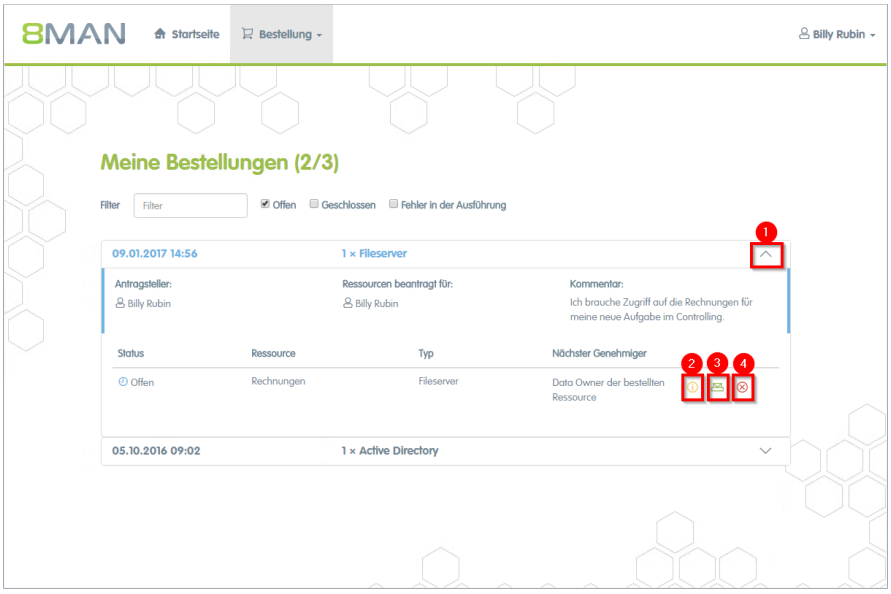
1. *Wählen Sie eine Zugriffskategorie.*
2. *Klicken Sie auf "In den Warenkorb legen".*



Fügen Sie ggf. weitere Ressourcen Ihrem Antrag hinzu. Klicken Sie auf "Warenkorb".



1. *Löschen Sie Positionen aus Ihrer Bestellung.*
2. *Fügen Sie Empfänger zu Ihrer Bestellung hinzu. Sie können für andere Benutzer den Zugriff bestellen.*
3. *Entfernen Sie Empfänger. Sie können auch sich selbst entfernen und nur für andere Benutzer bestellen.*
4. *Sie müssen einen Kommentar eingeben.*
5. *Starten Sie den Antrag.*



Nach einer Bestätigung zeigt 8MAN Ihnen eine Übersicht Ihrer Bestellungen.

1. *Klappen Sie die Detailansicht zu einer Bestellung auf oder zu.*
2. *Sehen Sie sich weitere Details an.*
3. *Versenden Sie erneut eine Benachrichtigungs-E-Mail an den Genehmiger.*
4. *Stornieren Sie Ihre Bestellung.*

7.4.3 Gruppenmitgliedschaften beantragen

Hintergrund / Mehrwert

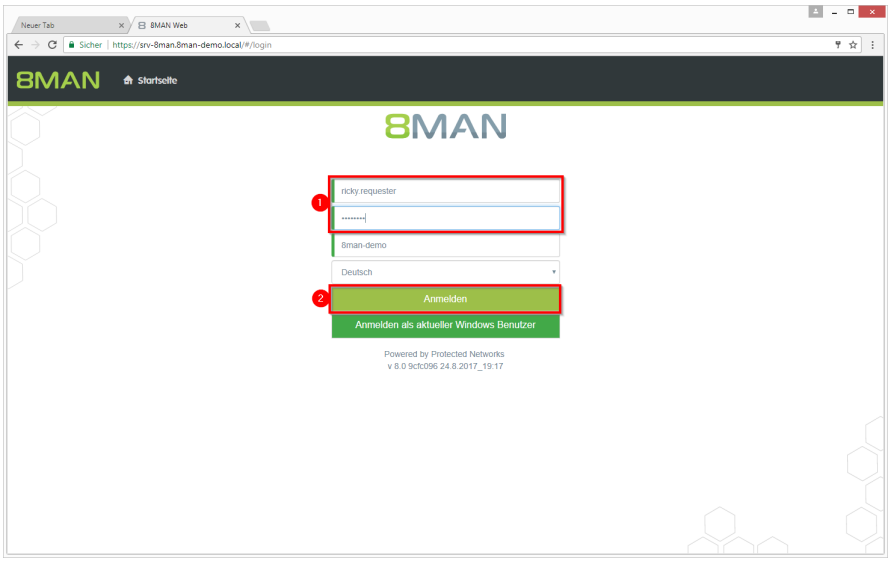
Im 8MATE GrantMA Self-Service-Portal bestellen Mitarbeiter Gruppenmitgliedschaften (z.B. für Rollengruppen) bei Data Owners oder Ressourcenverantwortlichen. Damit wird Access Rights Management zu einem kurzen, kontrollierbaren und dokumentierten Prozess.

Je nach Sicherheitslevel definieren Sie unterschiedlich komplexe Freigabeprozesse und involvieren die relevanten Entscheider.

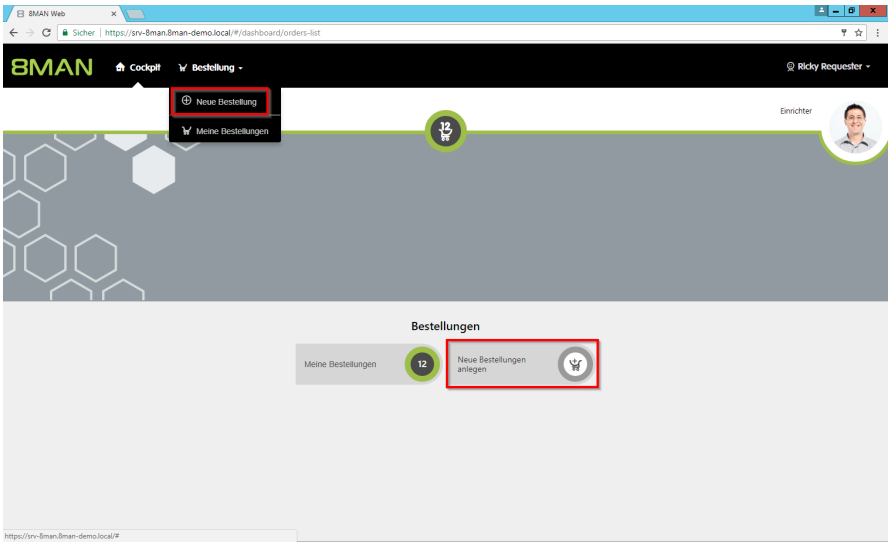
Weiterführende Services

Individuelle Freigabeworkflows definieren (Administrator)

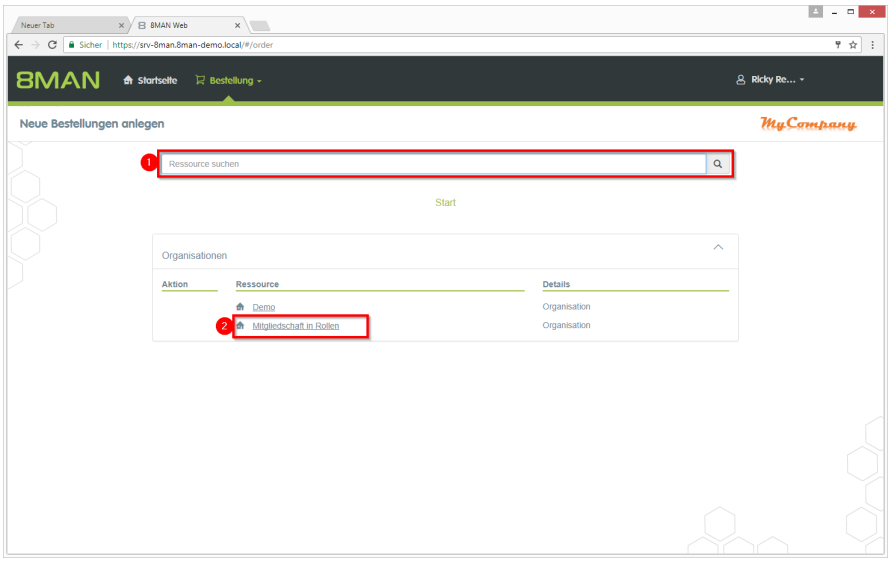
Der Prozess in einzelnen Schritten



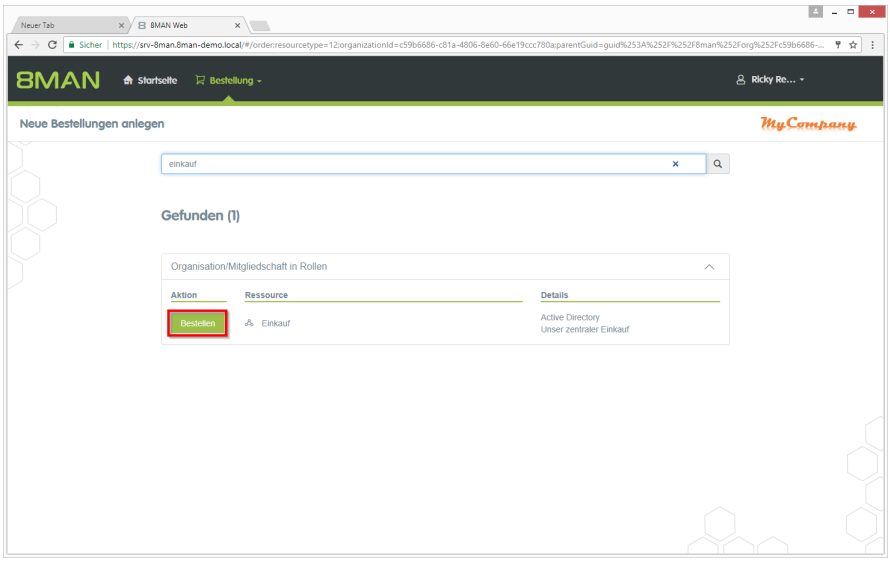
1. *Geben Sie Benutzername und Kennwort ein.*
2. *Klicken Sie auf "Anmelden".*



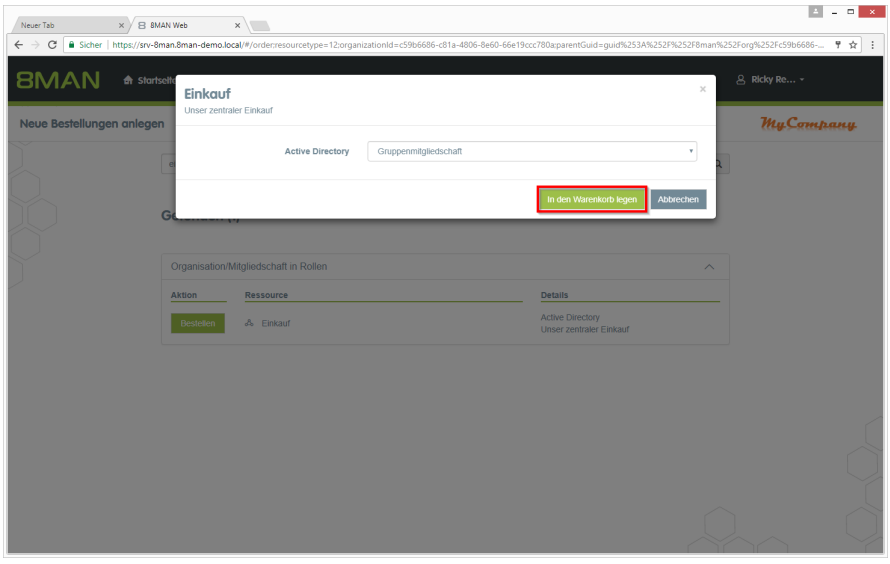
Klicken Sie auf "Neue Bestellung".



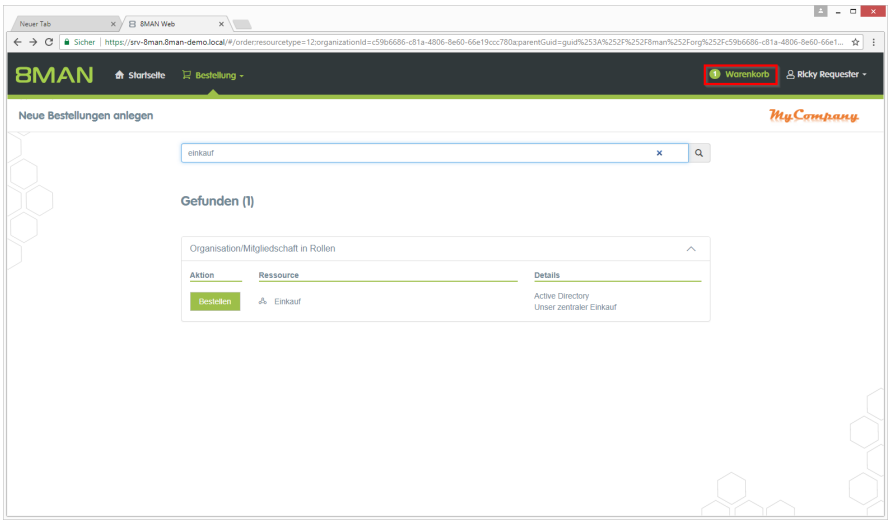
1. *Suchen Sie nach der Gruppe oder*
2. *navigieren Sie zur gewünschten Ebene.*



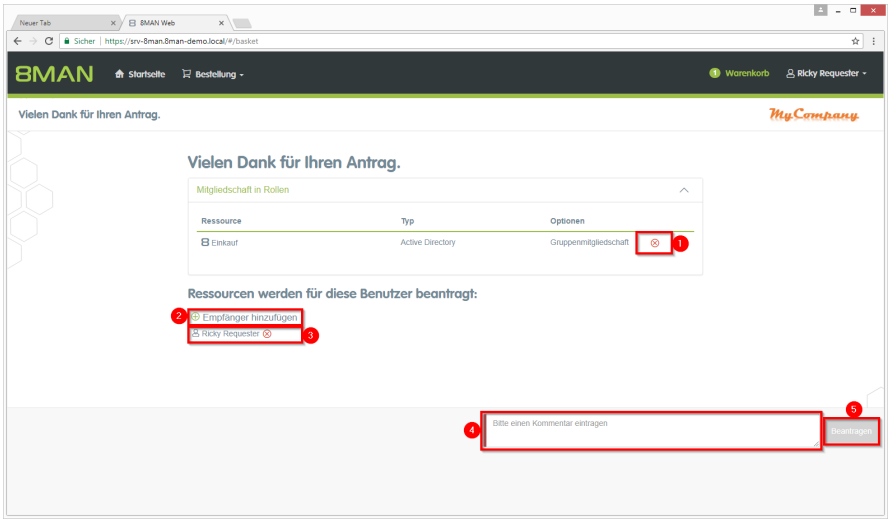
Haben Sie die gewünschte Ressource gefunden, klicken Sie auf "Bestellen".



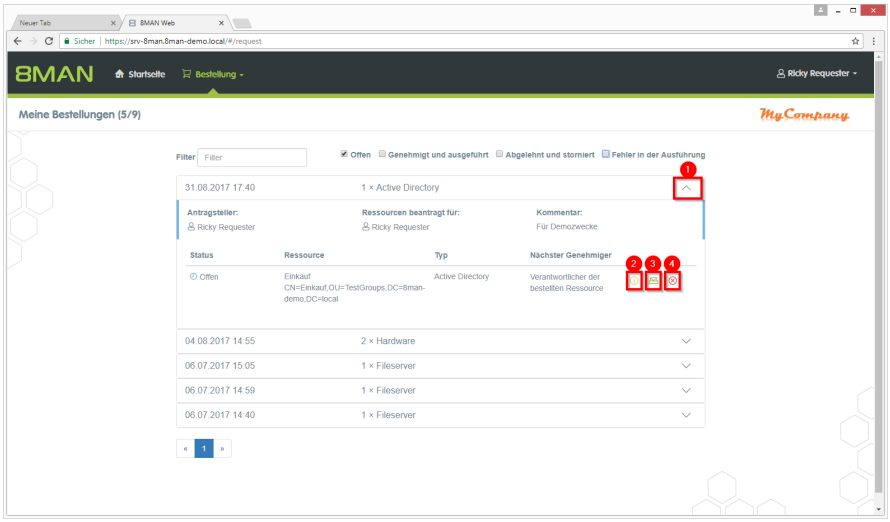
Klicken Sie auf "In den Warenkorb legen".



Fügen Sie ggf. weitere Ressourcen Ihrem Antrag hinzu. Klicken Sie auf "Warenkorb".



1. *Löschen Sie ggf. Positionen aus Ihrer Bestellung.*
2. *Fügen Sie Empfänger zu Ihrer Bestellung hinzu. Sie können für andere Benutzer den Zugriff bestellen.*
3. *Entfernen Sie Empfänger. Sie können auch sich selbst entfernen und nur für andere Benutzer bestellen.*
4. *Sie müssen einen Kommentar eingeben.Tragen Sie einen triftigen Grund ein. Der Kommentar wird dem Genehmiger im nächsten Schritt angezeigt.*
5. *Starten Sie den Antrag.*



Nach einer Bestätigung zeigt 8MAN Ihnen eine Übersicht Ihrer Bestellungen.

1. *Klappen Sie die Detailansicht zu einer Bestellung auf oder zu.*
2. *Sehen Sie sich weitere Details an.*
3. *Versenden Sie erneut eine Benachrichtigungs-E-Mail an den Genehmiger.*
4. *Stornieren Sie Ihre Bestellung.*

7.4.4 Neue Verzeichnisse bestellen

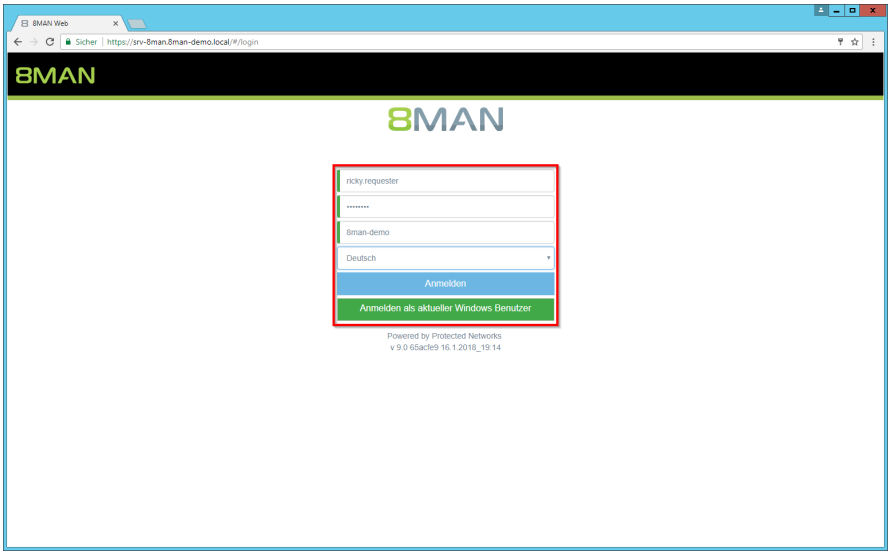
Hintergrund / Mehrwert

In der GrantMA können Sie ein neues Verzeichnis bestellen. Diese Funktion ist nützlich für Unternehmen, die restriktive Richtlinien zur Verzeichniserstellung verfolgen. Wir empfehlen, die Neuanlage von Verzeichnissen bis zur Ebene drei oder vier unterhalb der Freigabe nur nach Beantragung und Genehmigung zu ermöglichen.

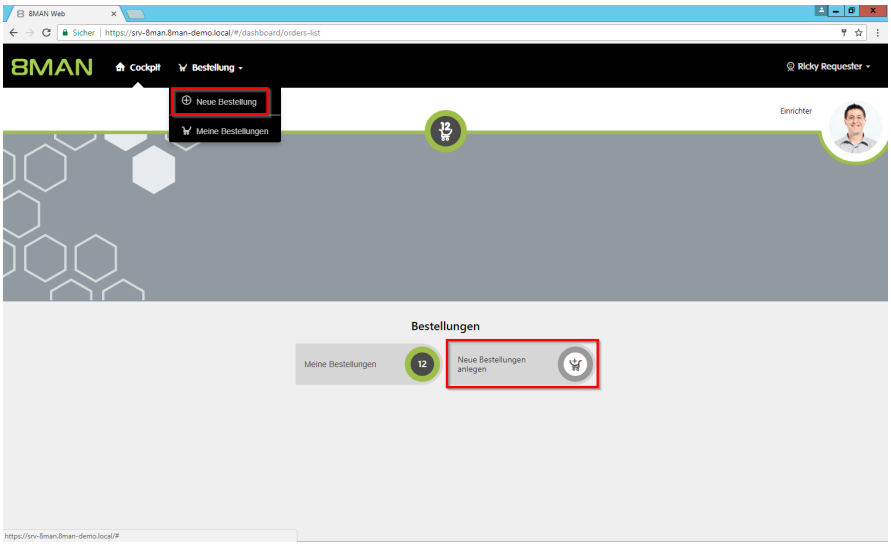
Weiterführende Services

Fileserver Rechte beim Data Owner bestellen

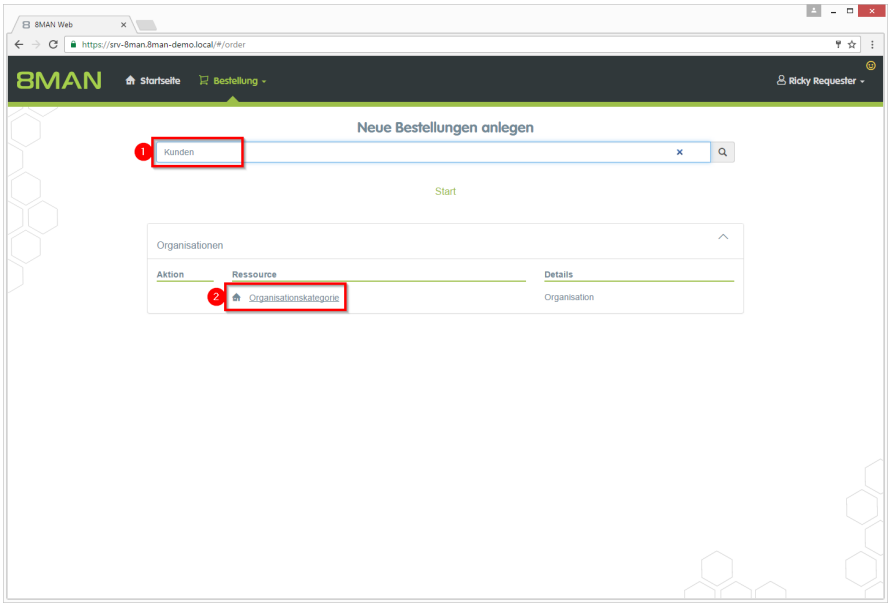
Der Prozess in einzelnen Schritten



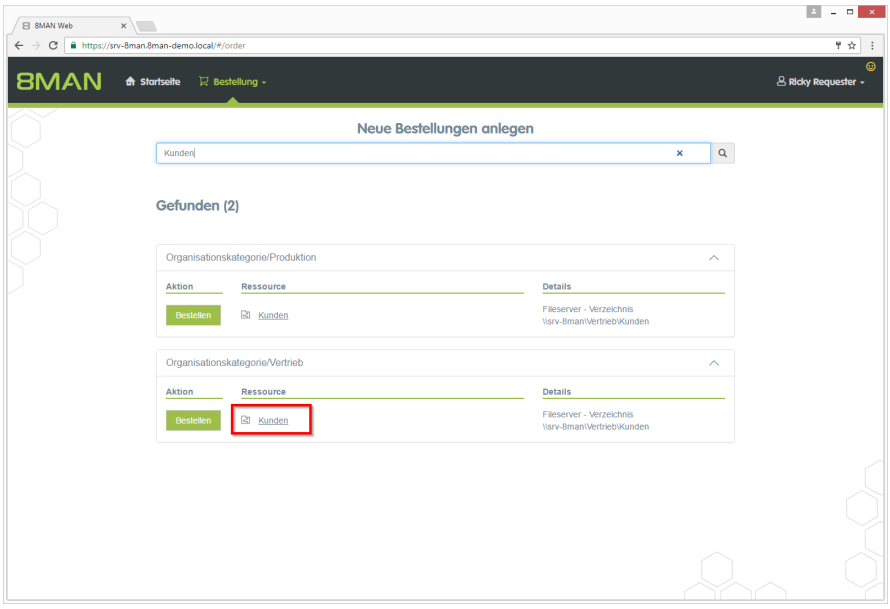
Loggen Sie sich als Besteller ein.



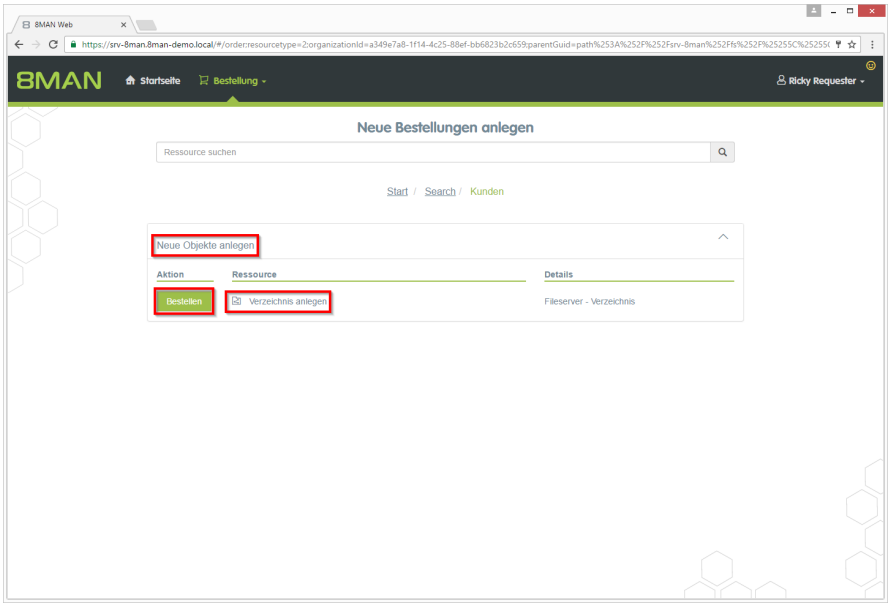
Starten Sie eine neue Bestellung.



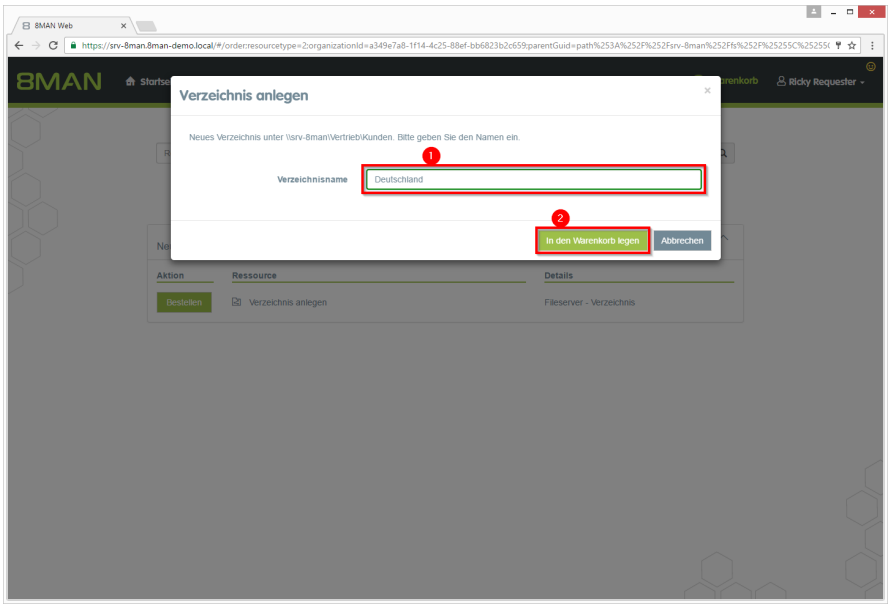
1. *Suchen Sie nach der gewünschten Ressource.*
2. *Alternativ: Navigieren Sie zur gewünschten Ressource.*



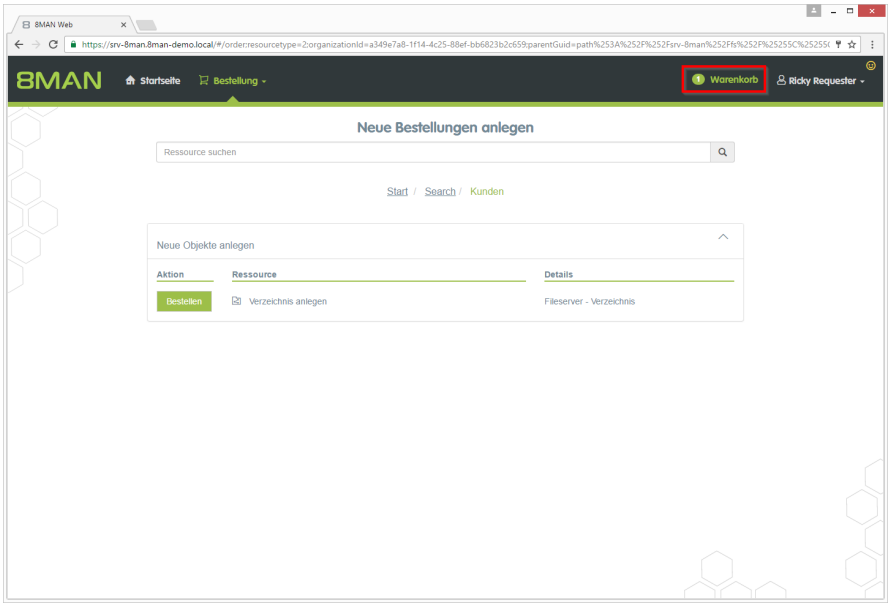
Klicken Sie auf das Suchergebnis.



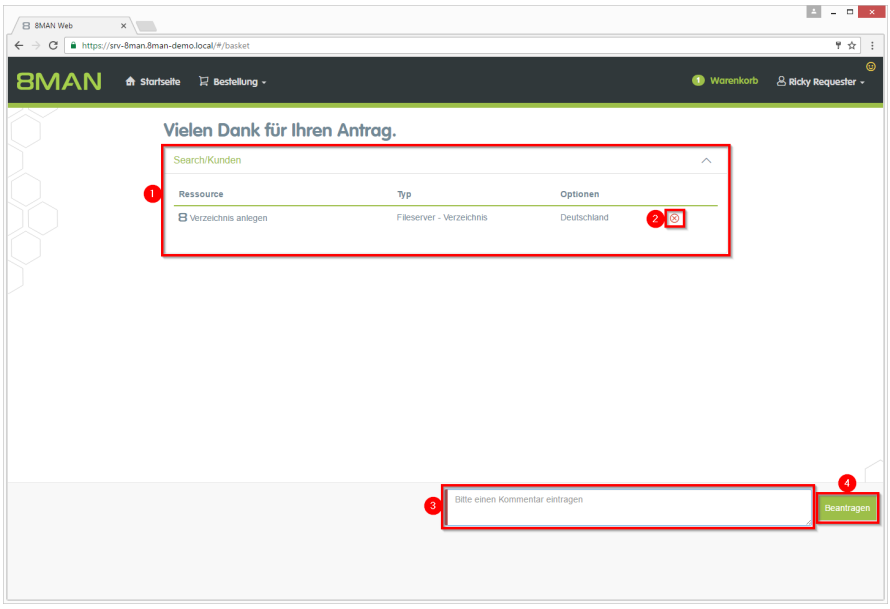
Im Bereich "Neue Objekte anlegen" Klicken Sie auf "Bestellen".



1. *Geben Sie dem neuen Verzeichnis einen Namen.*
2. *Legen Sie die Bestellung in den Warenkorb.*



Klicken Sie auf den Warenkorb.



1. *8MAN zeigt Ihnen den Warenkorb mit Ihrer Bestellung.*
2. *Alternativ: Löschen Sie Ihre Bestellung.*
3. *Sie müssen einen Kommentar eingeben, z.B. eine Ticketnummer.*
4. *Schließen Sie Ihre Bestellung ab.*

8MAN erstellt das neue Verzeichnis. Das neue Verzeichnis erbt alle Berechtigungen vom übergeordneten Verzeichnis.

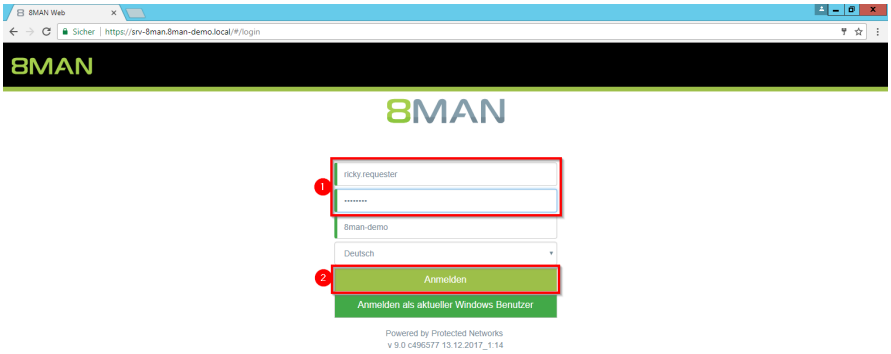
7.4.5 Als HR Mitarbeiter beim Help Desk ein Nutzerkonto erstellen lassen

Hintergrund / Mehrwert

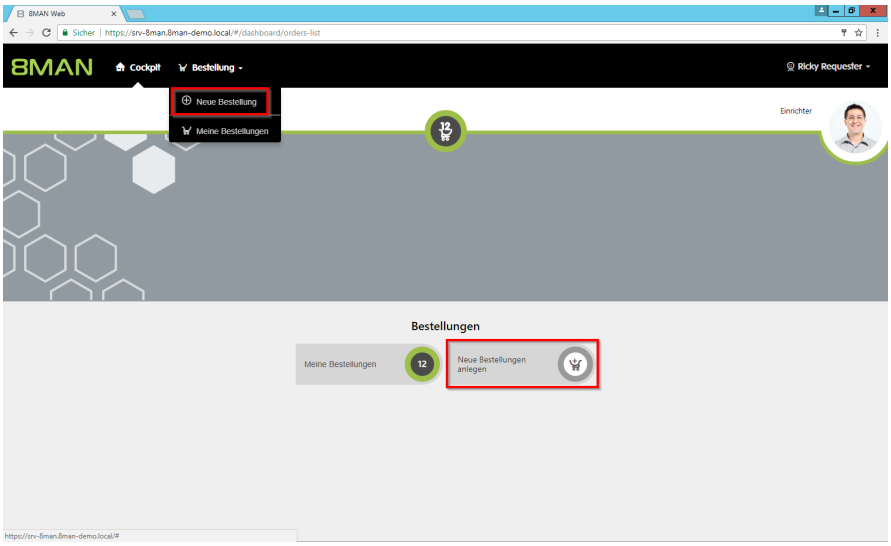
Im 8MATE GrantMA Self-Service-Portal können HR-Mitarbeiter Nutzerkonten für neue Mitarbeiter anlegen. Statt die Nutzerdaten an die IT zu senden, erfolgt die Eingabe und Erstellung in einem Schritt. Die IT gibt die automatische Erstellung nur noch frei.

Dieser Prozess eignet sich insbesondere für Abteilungen, die projektorientiert arbeiten und eine hohe Fluktuation aufweisen.

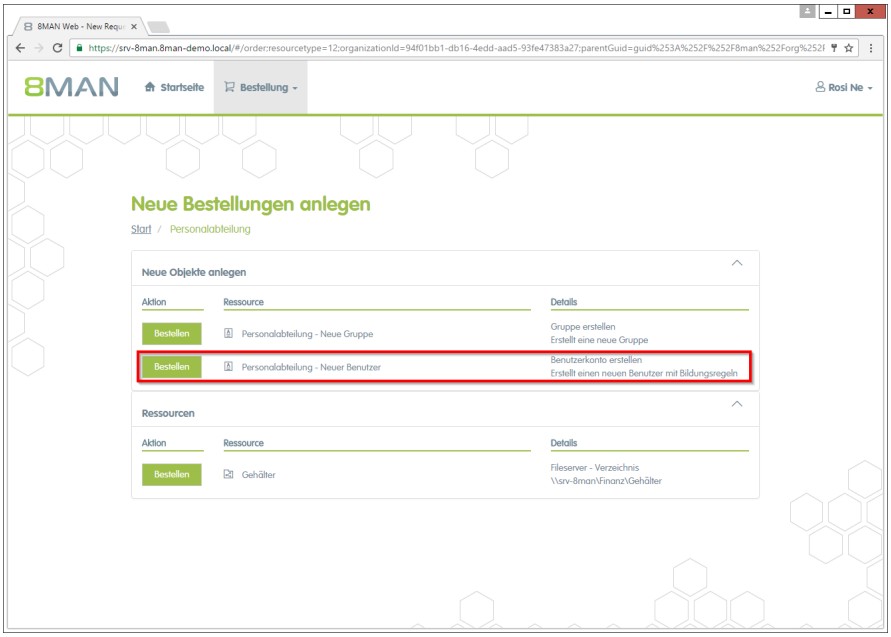
Der Prozess in einzelnen Schritten



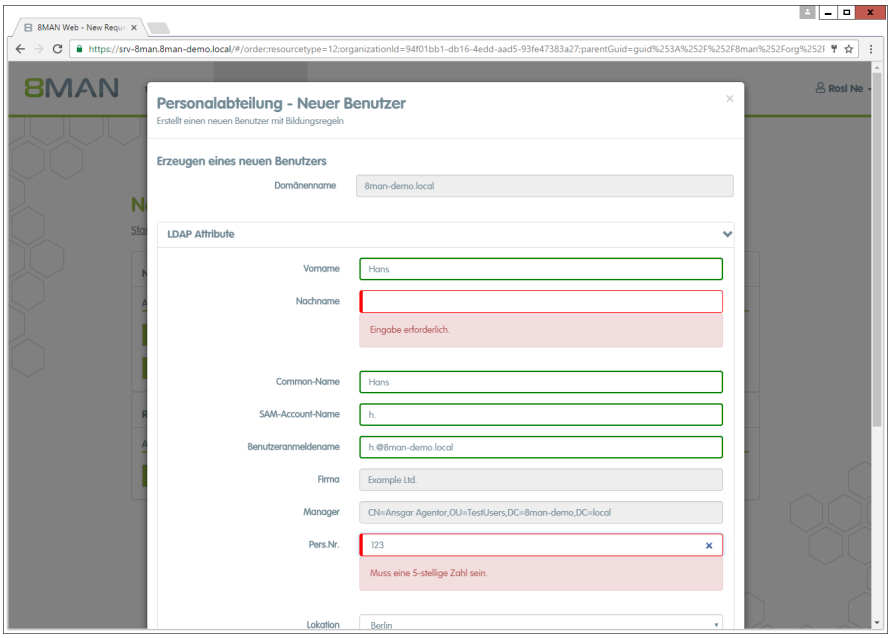
1. *Geben Sie Benutzername und Kennwort ein.*
2. *Klicken Sie auf "Anmelden".*



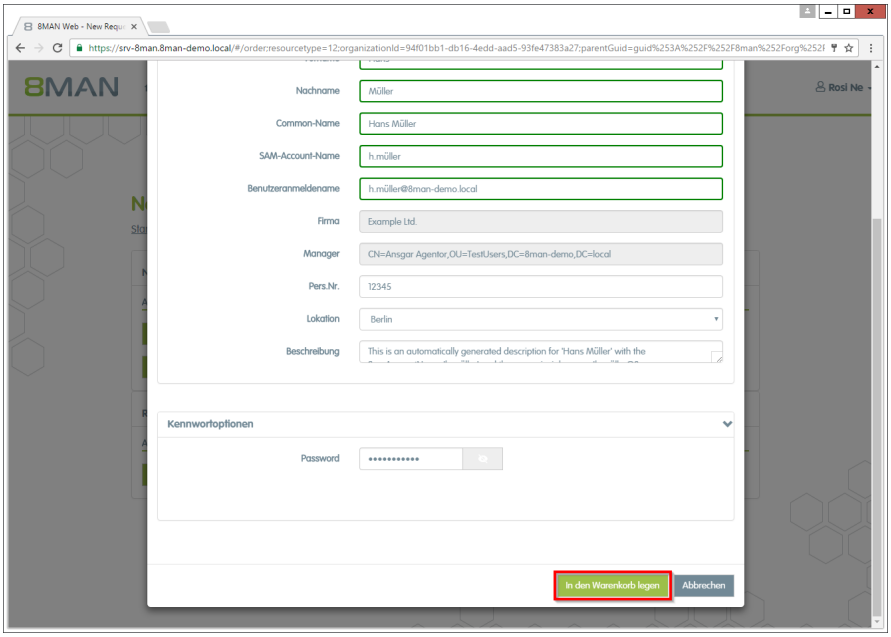
Klicken Sie auf "Neue Bestellung".



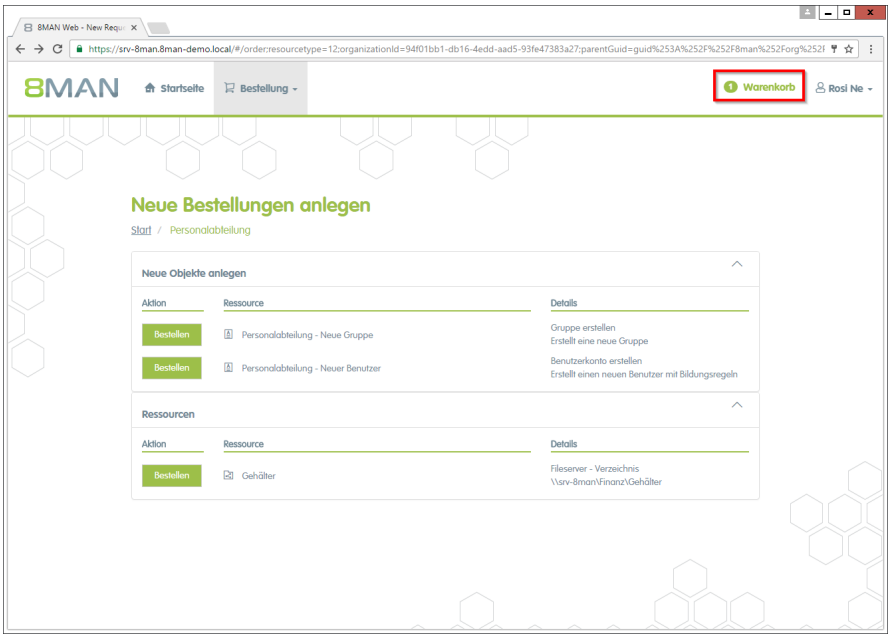
Wählen Sie "Neuer Benutzer" und klicken Sie auf bestellen.



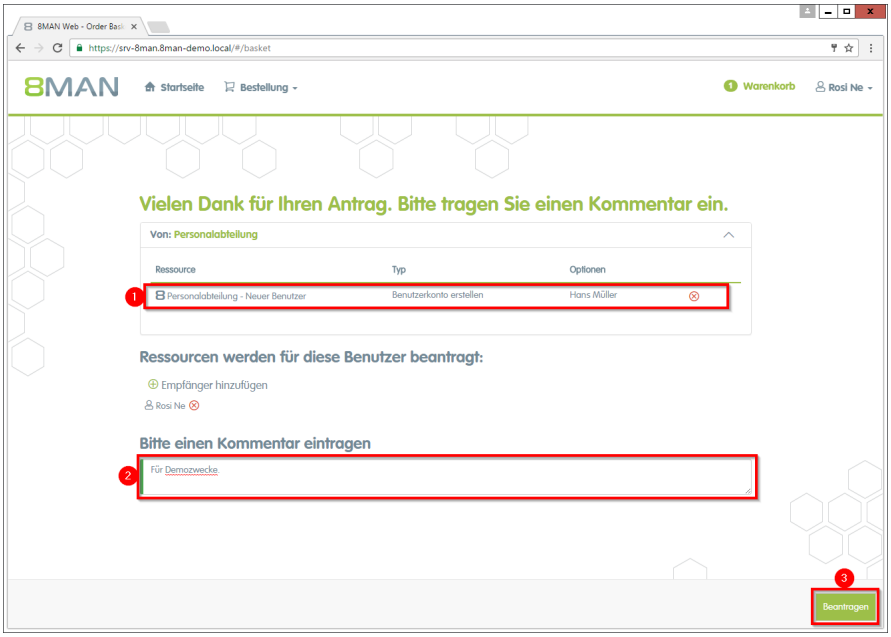
Geben Sie die Daten des neuen Benutzers ein. Rot markierte Felder sind Pflichtfelder bzw. ungültige Eingaben.



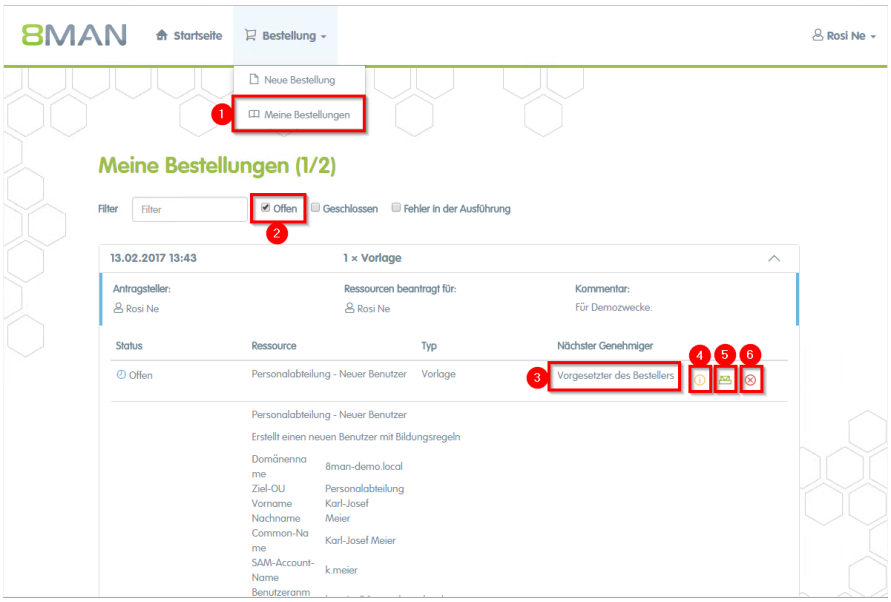
Nachdem Sie alle Daten eingegeben haben, klicken Sie auf "In den Warenkorb legen".



Fügen Sie ggf. weitere Ressourcen Ihrem Antrag hinzu. Klicken Sie auf "Warenkorb".



1. *Löschen Sie ggf. Positionen aus Ihrem Antrag.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie Ihre Bestellung.*



1. *Wählen Sie "Meine Bestellungen", um sich alle Ihre Bestellungen auflisten zu lassen.*
2. *Filtern Sie nach "Offen".*
3. *Sie sehen, welcher Genehmiger im nächsten Schritt zustimmen muss.*
4. *Lassen Sie sich weitere Details anzeigen.*
5. *Versenden Sie erneut eine Benachrichtigungs-E-Mail an den Genehmiger.*
6. *Stornieren Sie Ihre Bestellung.*

7.4.6 Skriptbasierte Services im GrantMA Self-Service-Portal bestellen

Hintergrund / Mehrwert

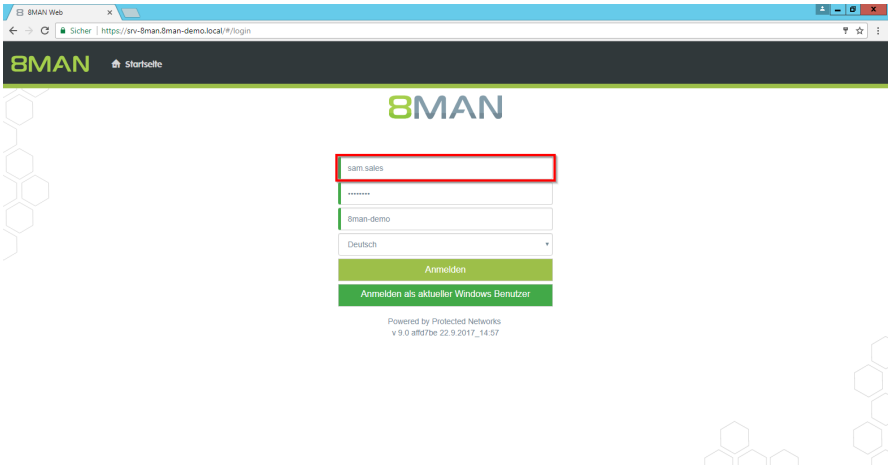
Neben der Bestellung von Nutzerkonten, Berechtigungen, Verzeichnissen oder frei definierbaren Objekten (Open Order) sind jetzt weitere skriptbasierte Services über den Webclient bestellbar.

Die IT definiert einen Service, der sich über ein Skript ausführen lässt. Der Service bekommt einen aussagekräftigen Namen (z.B. „Eine Projektstruktur auf dem Fileserver bestellen“). Der Mitarbeiter bestellt in der GrantMA den Service und gibt über ein Template die Basisdaten dazu ein. Nach dem individuell konfigurierbaren Freigabeworkflow wird das Skript automatisch gestartet.

Weiterführende Services

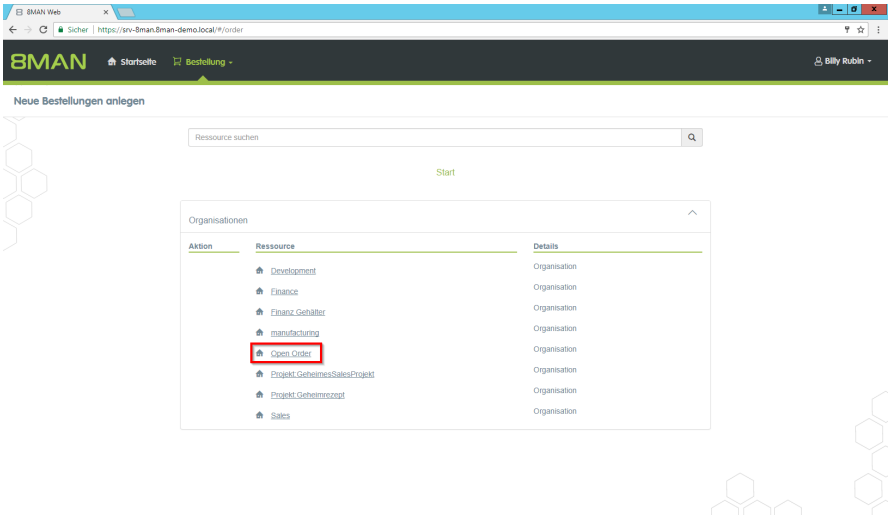
Einen skriptbasierten Service zur Bestellung konfigurieren (Administrator)

Der Prozess in einzelnen Schritten

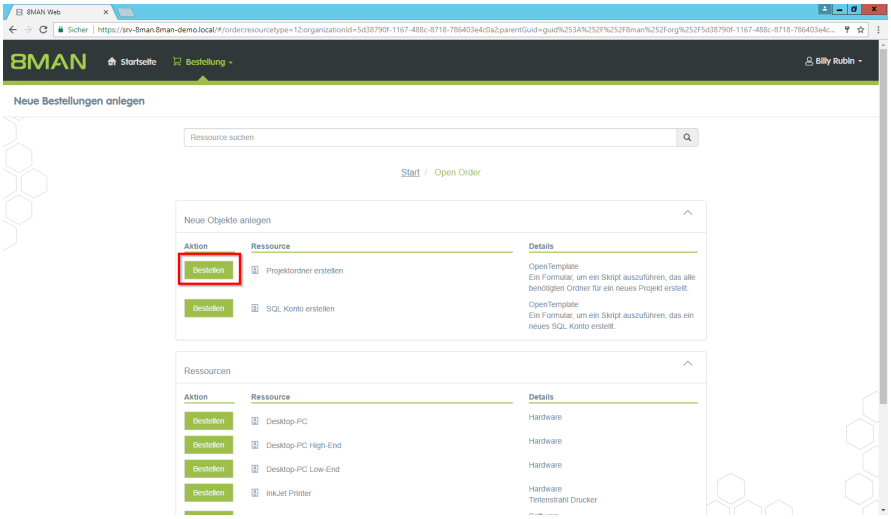


In dem folgenden Beispiel wird eine Projektordnerstruktur bestellt.

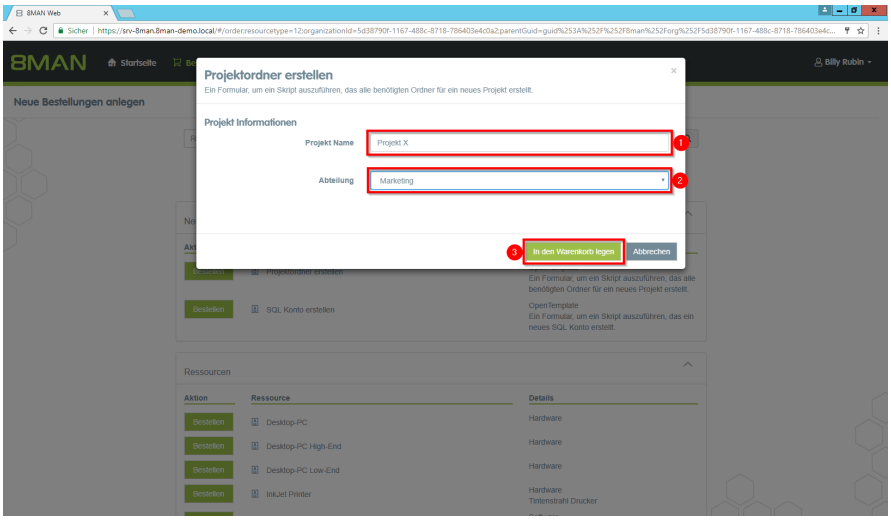
Loggen Sie sich als Besteller in den Webclient ein.



Wählen Sie die Organisationskategorie, die den Service enthält. Im Beispiel hier "Open Order".

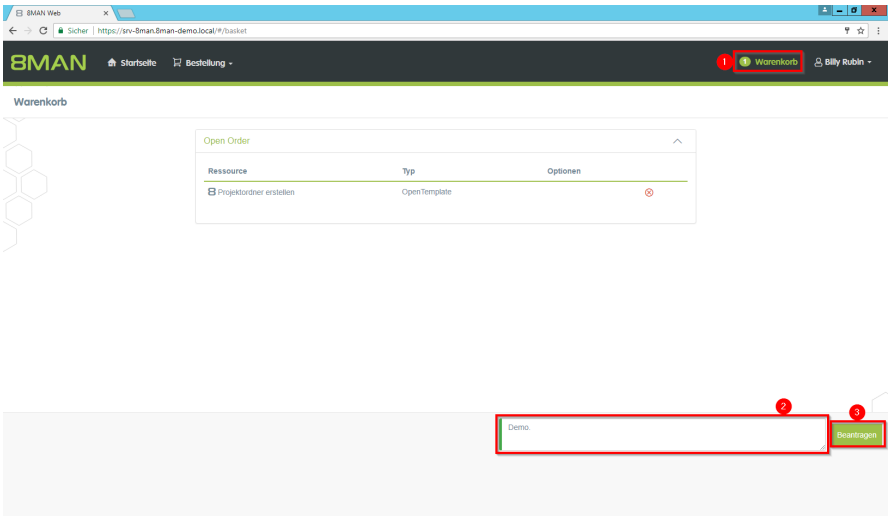


Wählen sie den Service "Projektordner erstellen" und klicken auf "Bestellen".



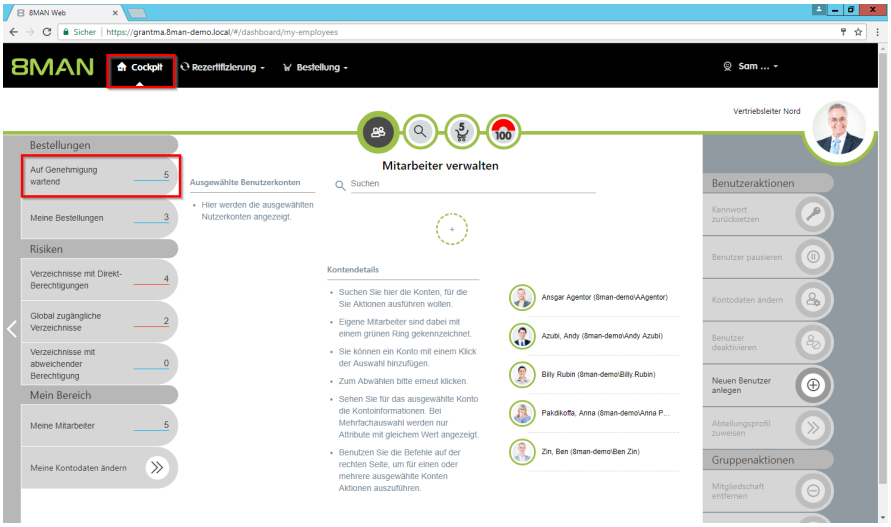
Geben Sie die Parameter zur Übergabe an das Skript ein. In dem Beispiel:

1. *Vergeben Sie einen Namen für den Projektordner.*
2. *Wählen Sie eine Abteilung. In dem Beispiel der "Elternordner", unter dem die Projektstruktur angelegt wird.*
3. *Klicken Sie auf "In den Warenkorb legen".*



Schließen Sie die Bestellung ab:

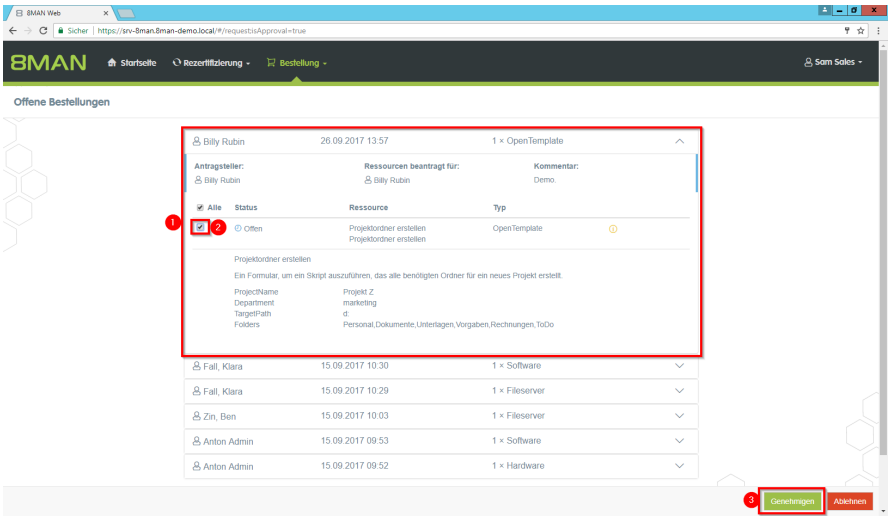
1. *Klicken Sie auf "Warenkorb".*
2. *Geben Sie einen Kommentar ein.*
3. *Klicken Sie auf "Beantragen".*



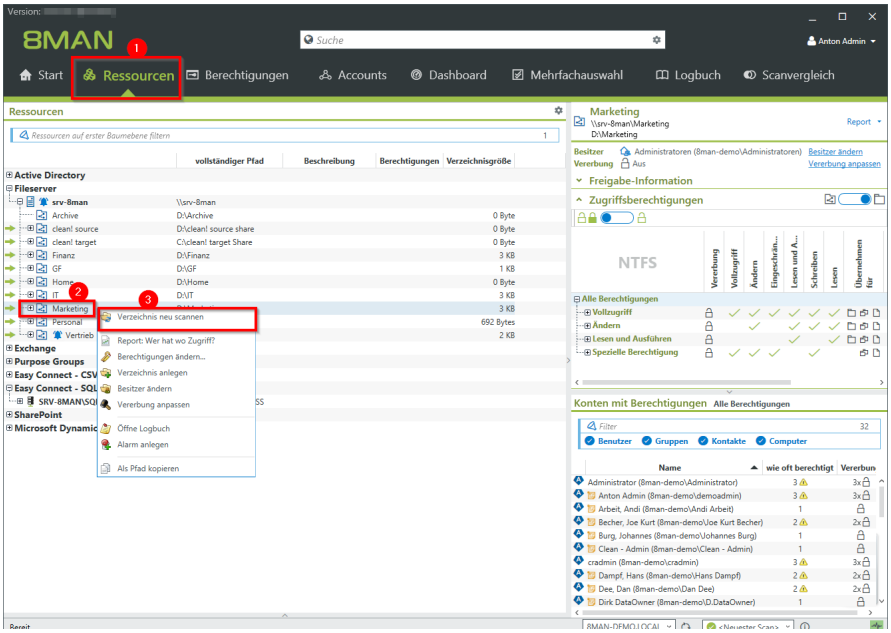
In dem hier gewählten Beispiel muss der Antrag durch Sam Sales genehmigt werden.

Melden Sie sich als Genehmiger an.

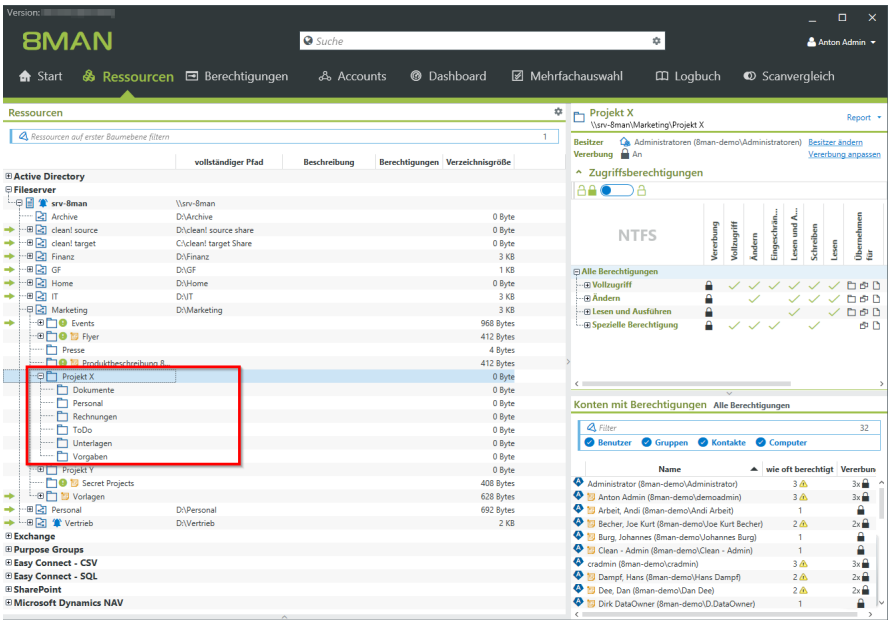
Klicken Sie auf "Auf Genehmigung wartend" .



1. *Wählen Sie die zuvor erstellte Bestellung und klappen sie auf.*
2. *Setzen Sie den Haken.*
3. *Klicken Sie auf "Genehmigen".*



Die Ordnerstruktur wird per Skript "außerhalb" von 8MAN erzeugt. Damit die neuen Ordner sichtbar werden, muss das entsprechende Verzeichnis neu gescannt werden.



Die bestellte, neu erzeugte Ordnerstruktur.

7.5 +8MATE GrantMA Workflows für Data Owner / Administratoren

7.5.1 Bestellungen genehmigen oder ablehnen (Cockpit)

Hintergrund / Mehrwert

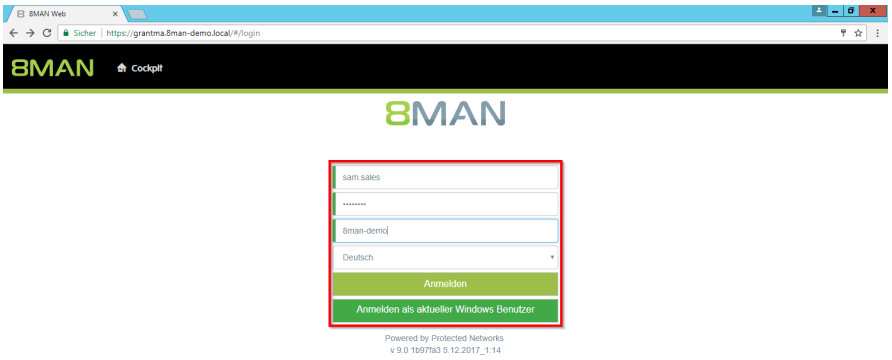
Je nachdem wie Sie den Freigabeprozess eingestellt haben, erhalten Sie Freigabeaufforderungen für die einzelnen Bestellprozesse. Damit behalten Sie als Administrator oder Data Owner die Prozesse im Auge.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen.

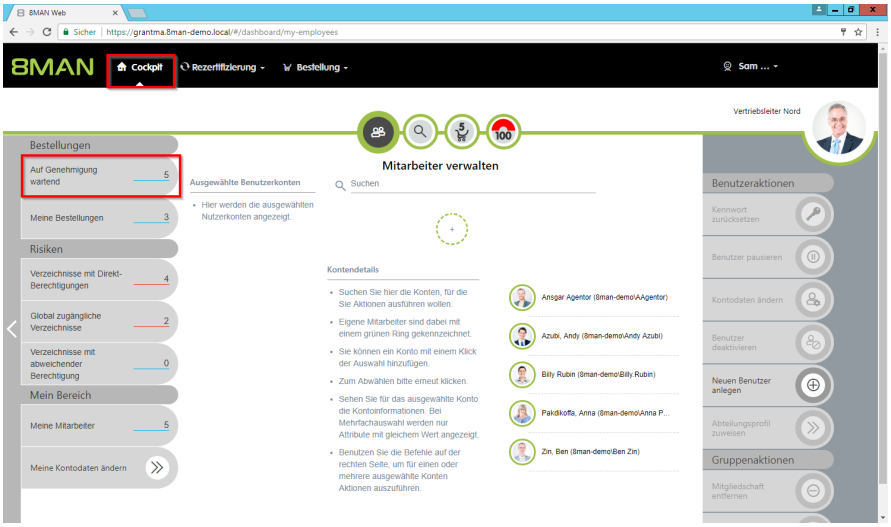
Weiterführende Services

Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

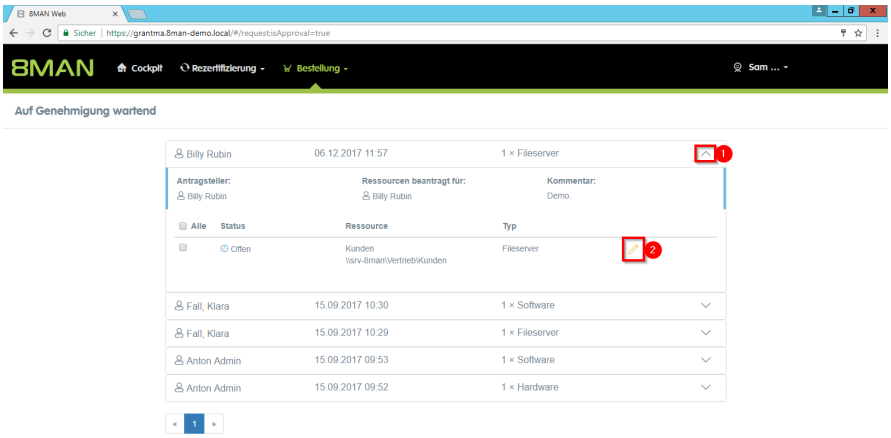


Melden Sie sich als Genehmiger an.

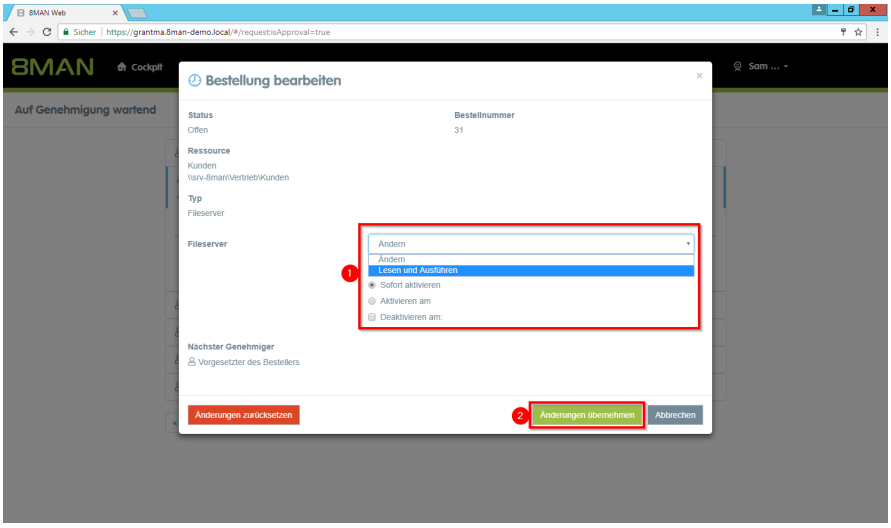


Klicken Sie auf "Auf Genehmigung wartend". In dem gezeigten Beispiel warten 5 Anträge auf Genehmigung.

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.

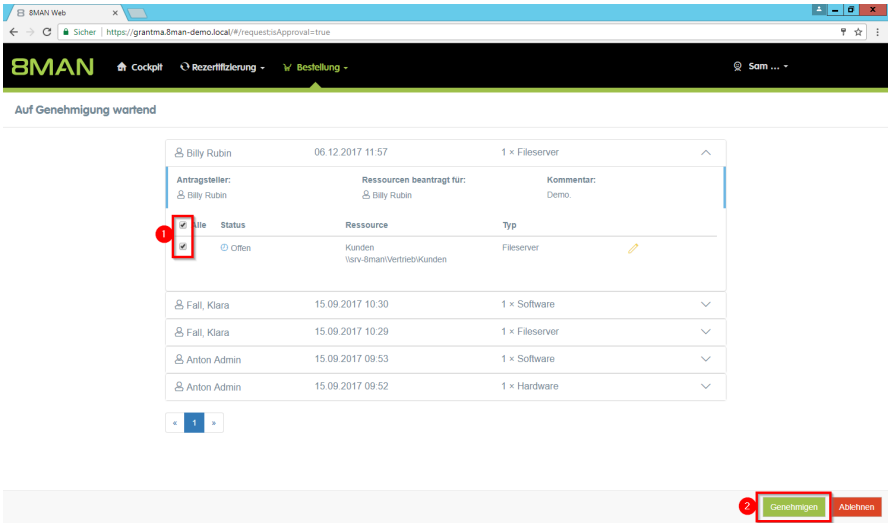


1. *Klappen Sie eine Bestellung auf, um die Positionen sehen zu können.*
2. *Lassen Sie sich Details zu den einzelnen Positionen einblenden.*
   Je nach Konfiguration sehen Sie ein Stift- oder ein Informationssysmbol.
   Stift: Sie können die Bestellung anpassen.
   Info: Sie sehen die Details.
   Klicken Sie auf das Stiftsysmbol.

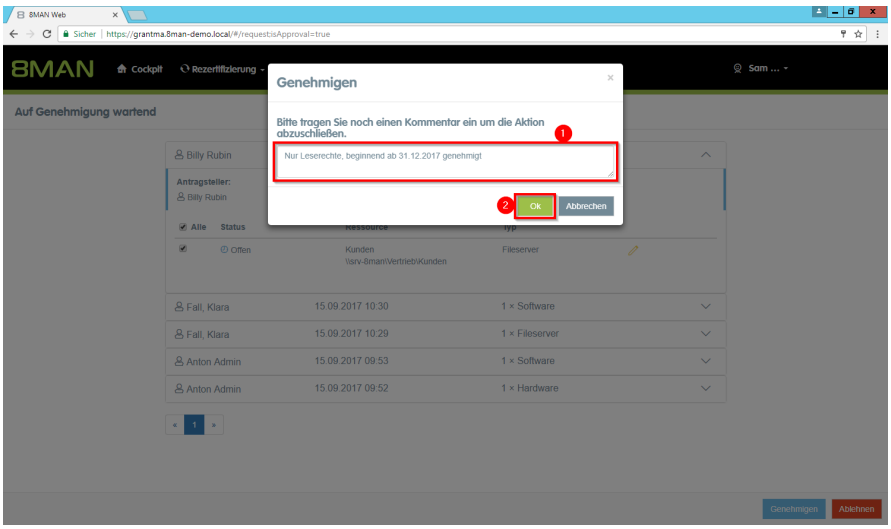


Sie können die Bestellanfrage bearbeiten.

1. *Zum Beispiel können Sie das angefragte "Ändern"- Recht auf "Lesen" zurückstufen und der Berechtigung ein Start- und Enddatum setzen.*
2. *Klicken Sie auf "Änderungen übernehmen".*



1. *Markieren Sie die gewünschte Bestellung oder Position.*
2. *Klicken Sie auf "Genehmigen".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Ok".*

Der Kommentar erscheint im Logbuch und ist damit revisionssicher dokumentiert.

7.5.2 Genehmiger automatisch über neue Anträge per E-Mail informieren

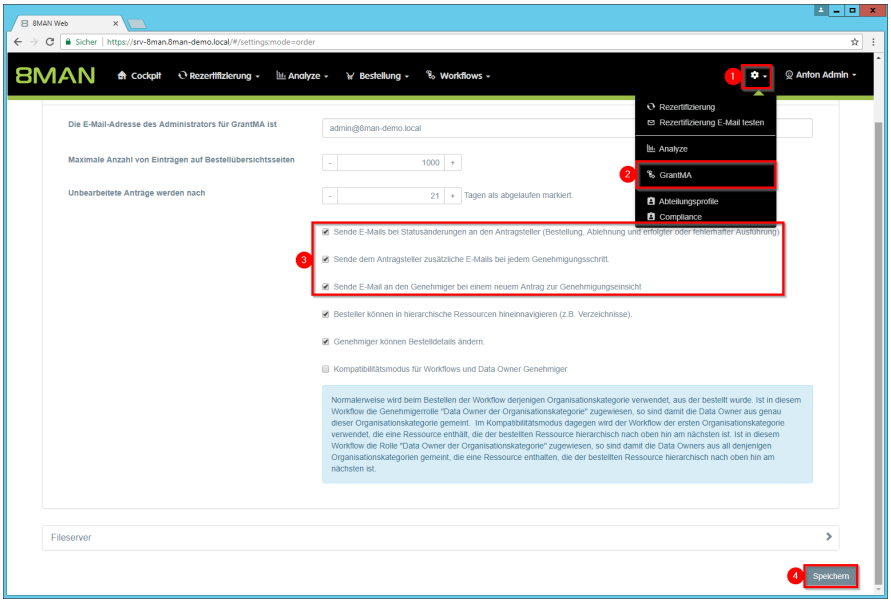
Hintergrund / Mehrwert

Damit Genehmiger nicht proaktiv neue Bestellanfragen auf der 8MAN Startseite prüfen müssen, empfehlen wir die Aktivierung von Freigabe E-Mails.

Weiterführende Services

Freigabeprozesse erstellen / ändern

Der Prozess in einzelnen Schritten



Loggen Sie sich als 8MAN Administrator in den Webclient ein.

1. *Klicken Sie auf das Zahnrad.*
2. *Klicken Sie auf "GrantMA".*
3. *Aktivieren Sie die E-Mail-Optionen. Damit sowohl der Antragssteller als auch Genehmiger auf dem Laufenden bleiben, empfehlen wir alle Optionen zu aktivieren.*
4. *Speichern Sie die Einstellungen.*

Genehmigung erforderlich

Sehr geehrte(r) cradmin,

Rosi Ne hat eine GrantMA Bestellung aufgegeben, die eine Genehmigung von Ihnen erfordert. Die Bestellung wurde am **15.11.2016** um **15:29** Uhr aufgegeben.

Auf der 8MATE GrantMA Seite können Sie die Bestellung genehmigen oder ablehnen.

Bestellübersicht

Rosi Ne schrieb den folgenden Bestellkommentar:
"Für Demozwecke."

Folgende Positionen wurden für

- **Rosi Ne**

bestellt:

Bestellnr.	Name	Typ	Optionen	Genehmigungshistorie
12	IT	Fileserver	Ändern	

Mit freundlichen Grüßen
8MATE GrantMA

Beispiel einer E-Mail-Benachrichtigung.

7.5.3 Eine Anfrage im Self Service Portal ablehnen oder bestätigen

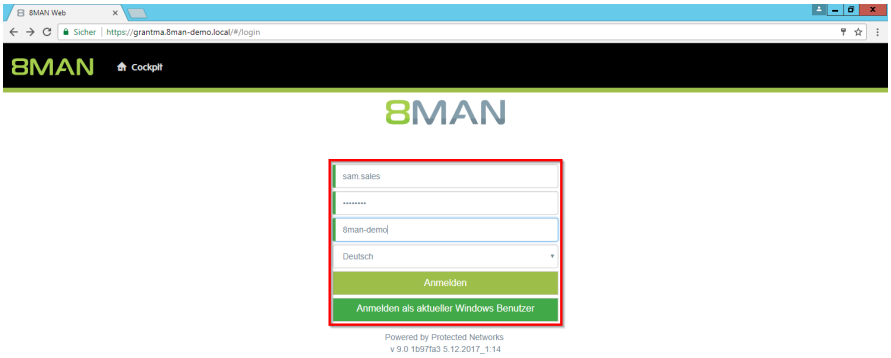
Hintergrund / Mehrwert

Je nachdem wie Sie den Freigabeprozess eingestellt haben, erhalten Sie Freigabeaufforderungen für die einzelnen Bestellprozesse. Damit behalten Sie als Administrator oder Data Owner die Prozesse im Auge.

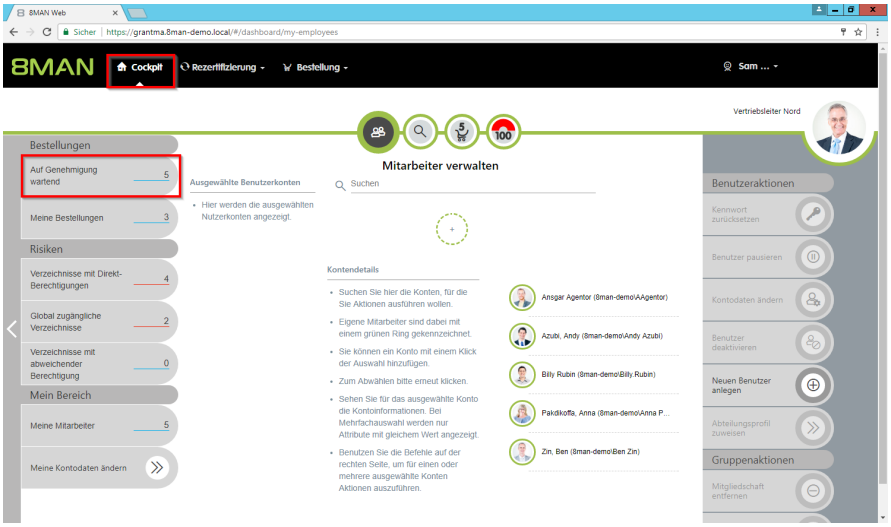
Weiterführende Services

Individuelle Freigabeworkflows definieren

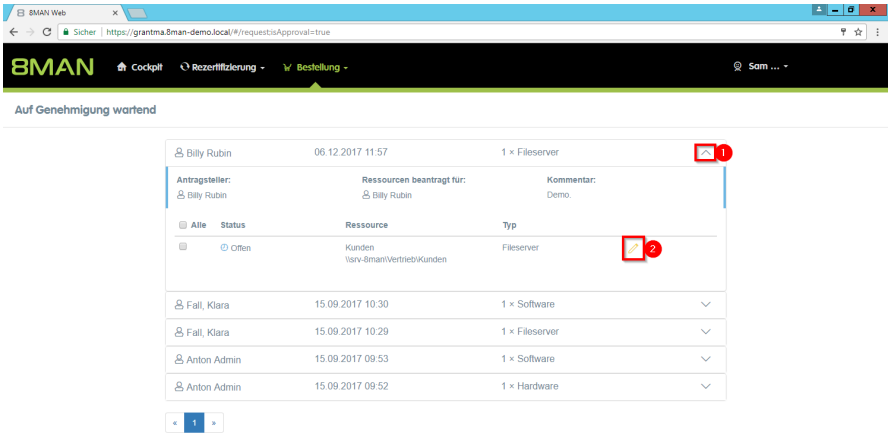
Der Prozess in einzelnen Schritten



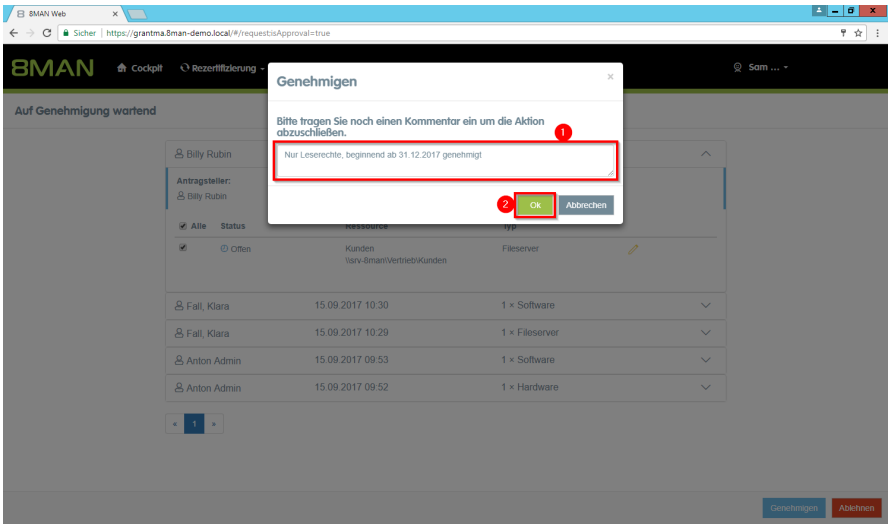
Melden Sie sich mit Ihrem Genehmiger-Zugang an.



Klicken Sie auf "Warten auf Genehmigung". In dem gezeigten Beispiel warten "2" Anträge auf Genehmigung.



1. *Klappen Sie eine Bestellung auf, um die Positionen sehen zu können.*
2. *Lassen Sie sich Details zu den einzelnen Positionen einblenden.*
3. *Selektieren Sie eine oder mehrere Positionen.*
4. *Klicken Sie auf "Genehmigen" oder "Ablehnen".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Ok".*

Der Kommentar erscheint im Logbuch und ist damit revisionssicher dokumentiert.

8. User Provisioning

8.1 Active Directory

8.1.1 Administrator

8.1.1.1 Ein Nutzerkonto anlegen

Hintergrund / Mehrwert

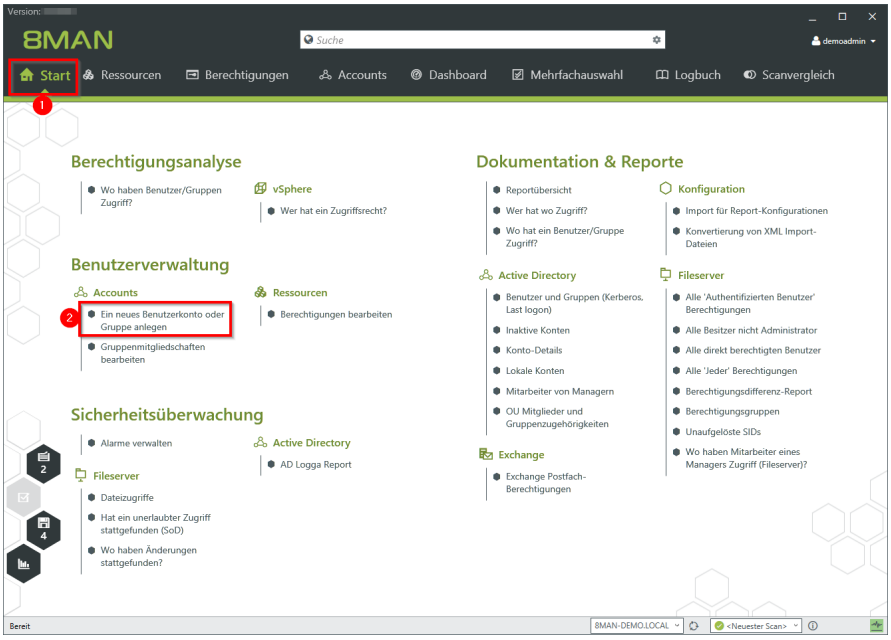
Mit 8MAN legen Sie schnell und standardisiert Nutzerkonten an. Sie können den Prozess an den Helpdesk delegieren und als Prozess über eigens erstellte Templates für unterschiedliche Unternehmensrollen spezifizieren.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen.

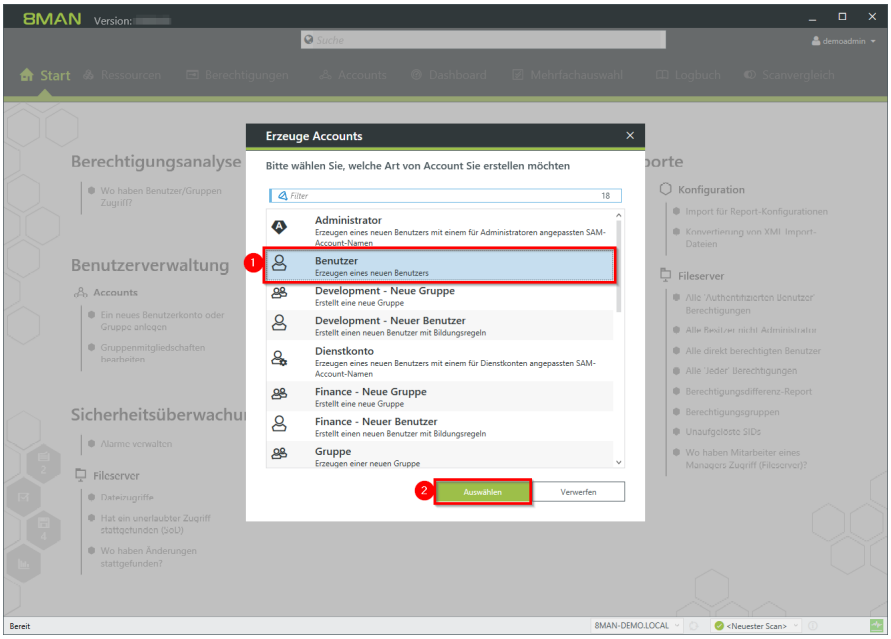
Weiterführende Services

Erstellung von angepassten Templates (siehe Handbuch Templates anpassen)

Der Prozess in einzelnen Schritten

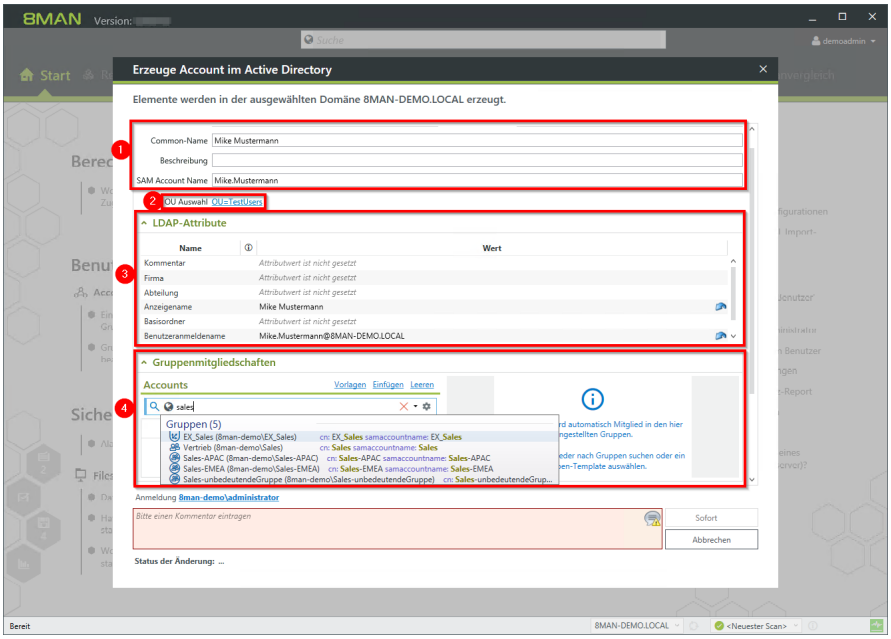


1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Ein neues Benutzerkonto oder Gruppe anlegen".*

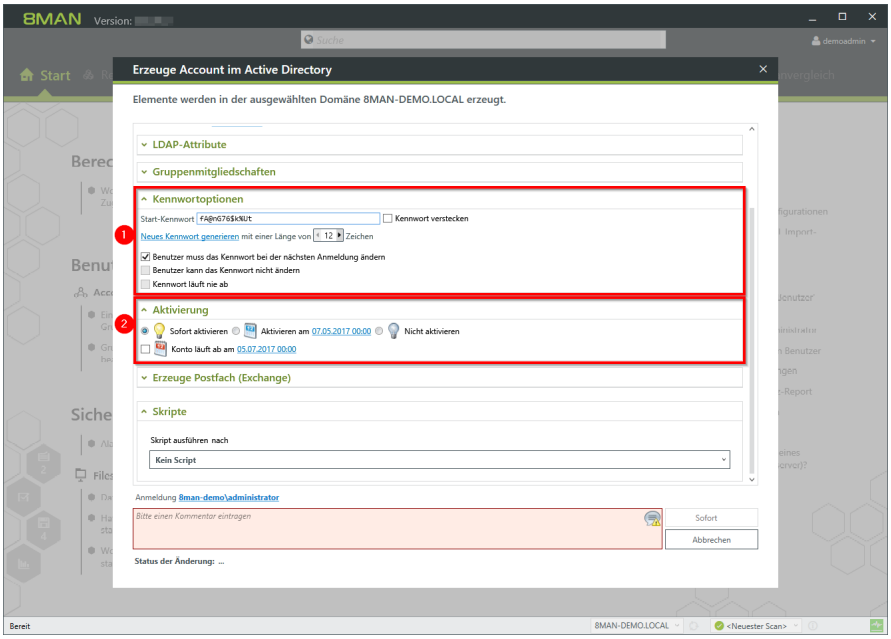


8MAN bietet nach Erstinstallation vier Standardvorlagen. Sie können unbegrenzt viele, an Ihre Bedürfnisse angepasste Vorlagen erstellen. Wir empfehlen, angepasste Vorlagen zu verwenden, da sich dadurch der Anlagevorgang vereinheitlichen und deutlich beschleunigen lässt.

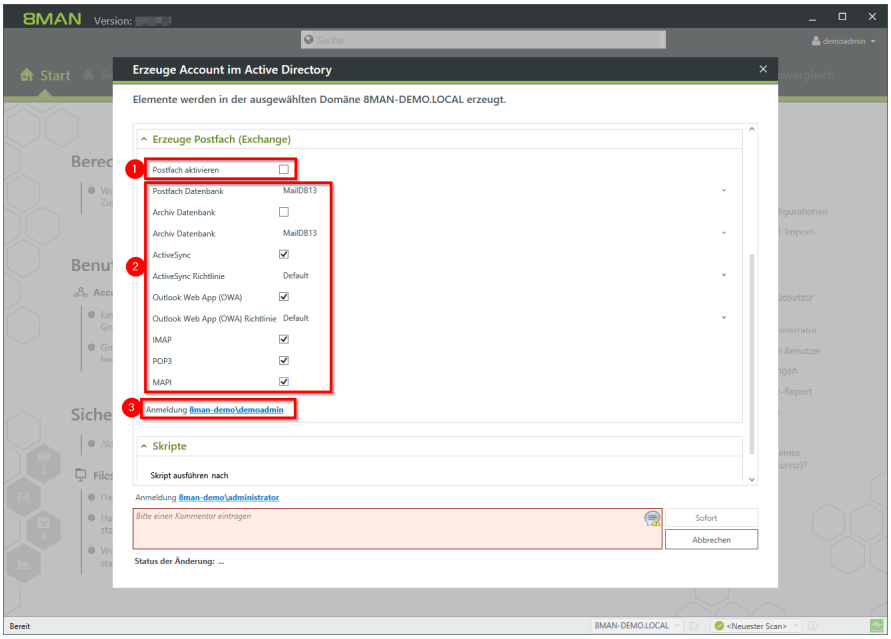
1. *Wählen Sie eine Benutzer-Vorlage.*
2. *Klicken Sie "Auswählen".*



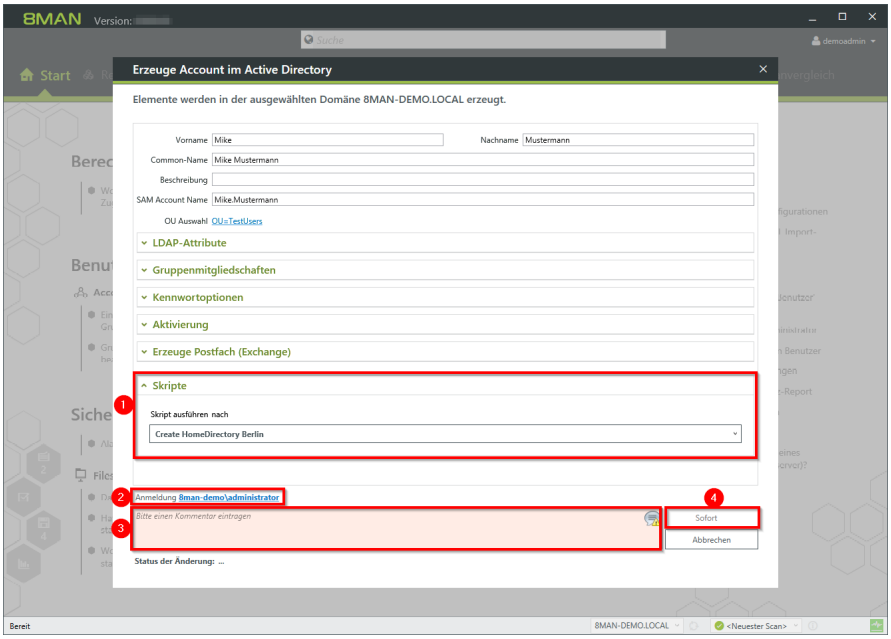
1. *Geben Sie die Stammdaten ein.*
2. *Ändern Sie ggf. die OU.*
3. *Ergänzen Sie weitere LDAP Attribute.*
4. *Sie können bereits bei der Nutzeranlage Gruppenmitgliedschaften festlegen.*



1. *Legen Sie die Kennwortoptionen fest.*
2. *Mit 8MAN können Sie die Aktivierung des Kontos terminieren und ein Ablaufdatum setzen.*



1. *Aktivieren Sie die Option, um für den Nutzer ein Postfach anzulegen.*
2. *Legen Sie Postfachoptionen fest.*
3. *Geben Sie an, mit welchen Anmeldeinformationen das Postfach erstellt werden soll.*



1. *Wählen Sie ein Skript aus, welches nach der Anlage des neuen Benutzers ausgeführt wird. Welche Skripte zur Auswahl stehen, legen Sie in der Skriptkonfiguration fest.*
2. *Geben Sie an, mit welchen Anmeldeinformationen das neue Konto im AD angelegt werden soll.*
3. *Sie müssen einen Kommentar eingeben.*

Sicherheitsrelevante Ereignisse wie die Erstellung eines Nutzerkontos sollten vom Ersteller immer begründet werden. Dies dient auch der eigenen Absicherung. Wir empfehlen, eine Ticketnummer und den Beauftrager zu hinterlegen.

4. *Starten Sie die Ausführung.*

8.1.1.2 Gruppen anlegen und Benutzer hinzufügen

Hintergrund / Mehrwert

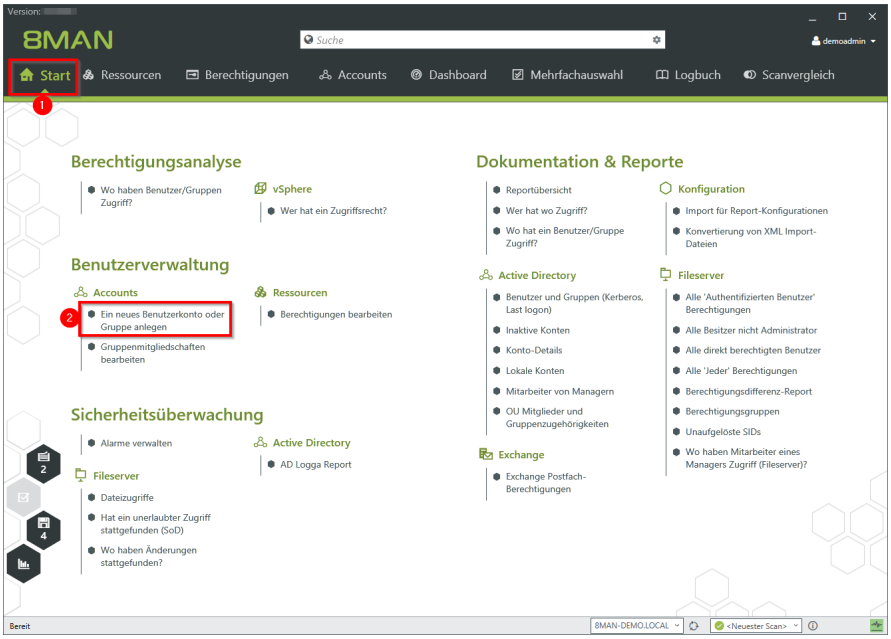
Mit 8MAN legen Sie schnell und standardisiert Gruppen an. Der Prozess wird automatisch dokumentiert.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen.

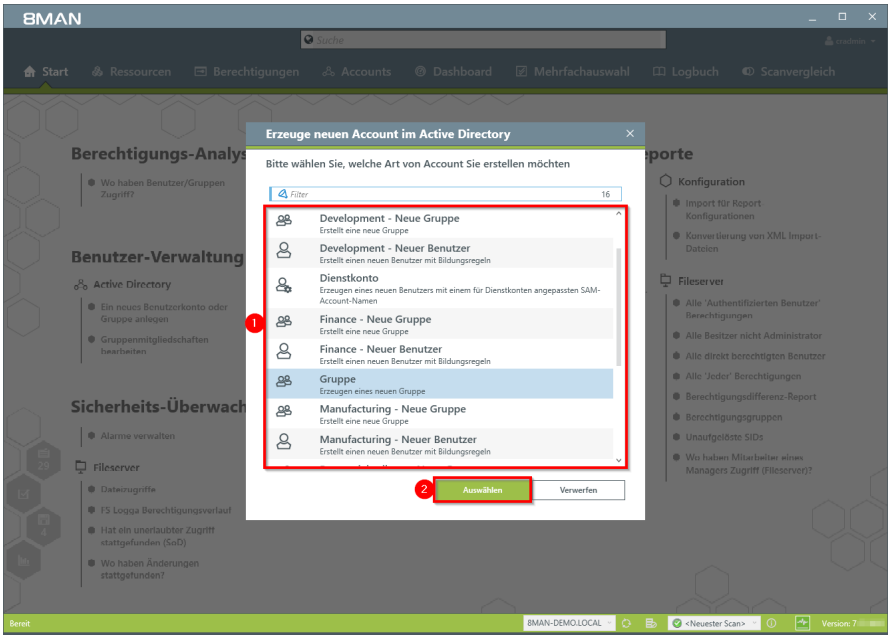
Weiterführende Services

Erstellung von angepassten Templates (siehe Handbuch Templates anpassen)
Gruppenmitgliedschaften bearbeiten

Der Prozess in einzelnen Schritten

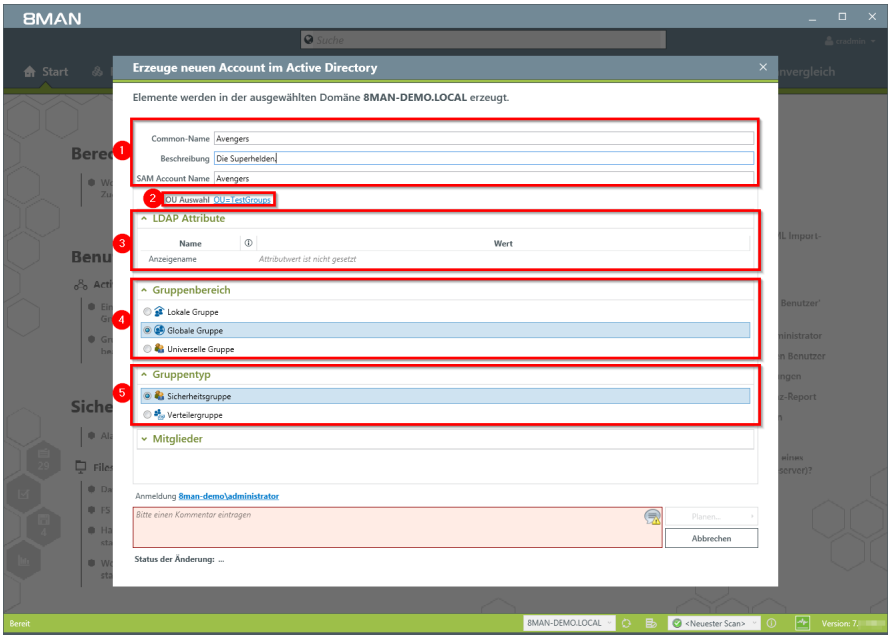


1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Ein neues Benutzerkonto oder Gruppe anlegen".*

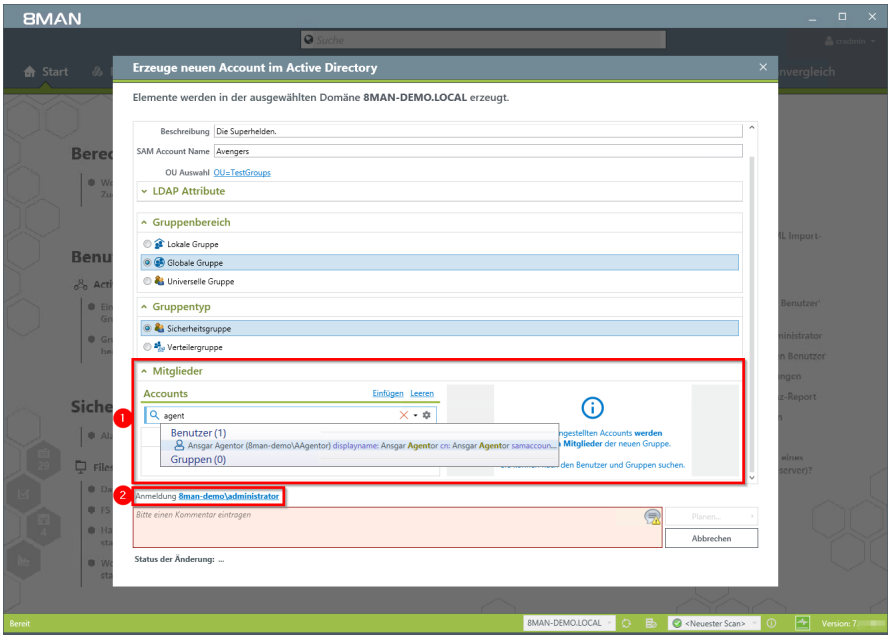


8MAN bietet nach Erstinstallation vier Standardvorlagen. Sie können unbegrenzt viele, an Ihre Bedürfnisse angepasste Vorlagen erstellen. Wir empfehlen, angepasste Vorlagen zu verwenden, da sich dadurch der Anlagevorgang vereinheitlichen und deutlich beschleunigen lässt.

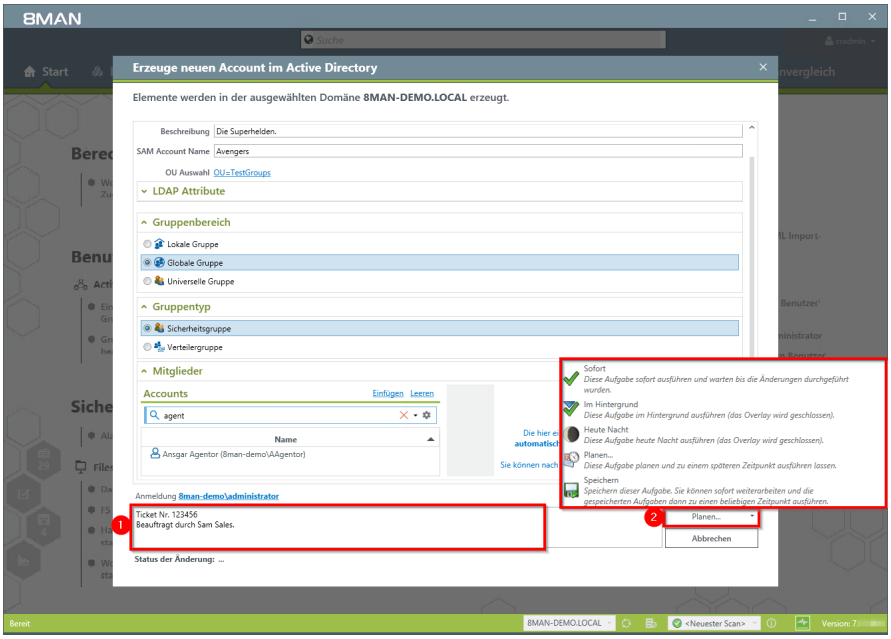
1. *Wählen Sie eine Gruppen-Vorlage.*
2. *Klicken Sie "Auswählen".*



1. *Geben Sie die Stammdaten ein.*
2. *Ändern Sie ggf. die OU.*
3. *Ergänzen Sie weitere LDAP Attribute.*
4. *Legen Sie den Gruppenbereich (group scope) fest.*
5. *Legen Sie den Gruppentyp fest.*



1. *Sie können bereits bei der Gruppenanlage Mitglieder festlegen.*
2. *Geben Sie an, mit welchen Anmeldeinformationen die neue Gruppe im AD angelegt wird.*



1. *Sie müssen einen Kommentar eingeben.*

Sicherheitsrelevante Ereignisse, wie die Erstellung eines Nutzerkontos sollten vom Ersteller immer begründet werden. Dies dient auch der eigenen Absicherung. Wir empfehlen, eine Ticketnummer und den Beauftrager zu hinterlegen.

2. *Führen Sie die Anlage sofort oder später aus, oder speichern Sie die Aufgabe und beenden sie später.*

8.1.1.3 Gruppenmitgliedschaften bearbeiten

Hintergrund / Mehrwert

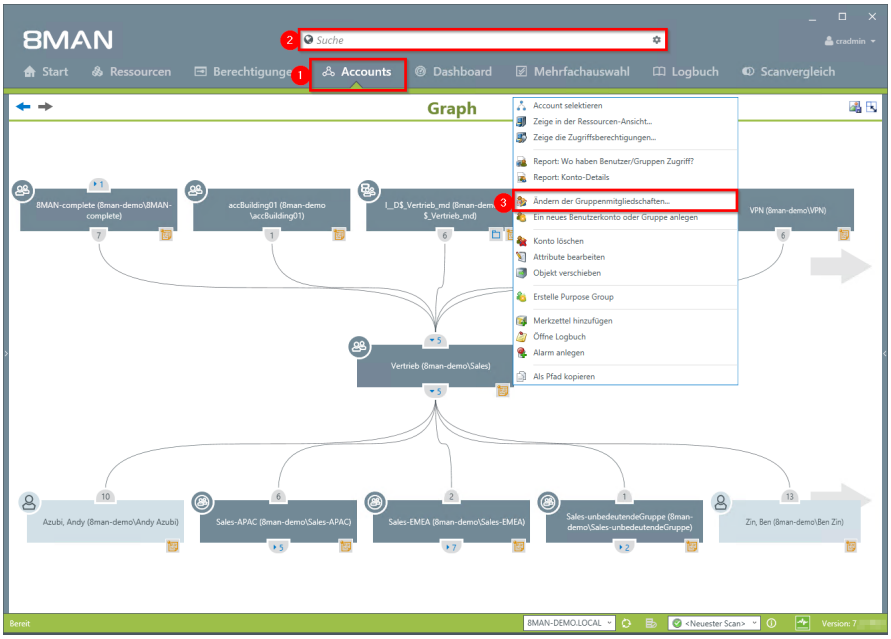
Mit 8MAN können Sie schnell Gruppenmitgliedschaften bearbeiten. Dabei sehen Sie auch gleich in welchen Gruppen die Gruppe Mitglied ist.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen.

Weiterführende Services

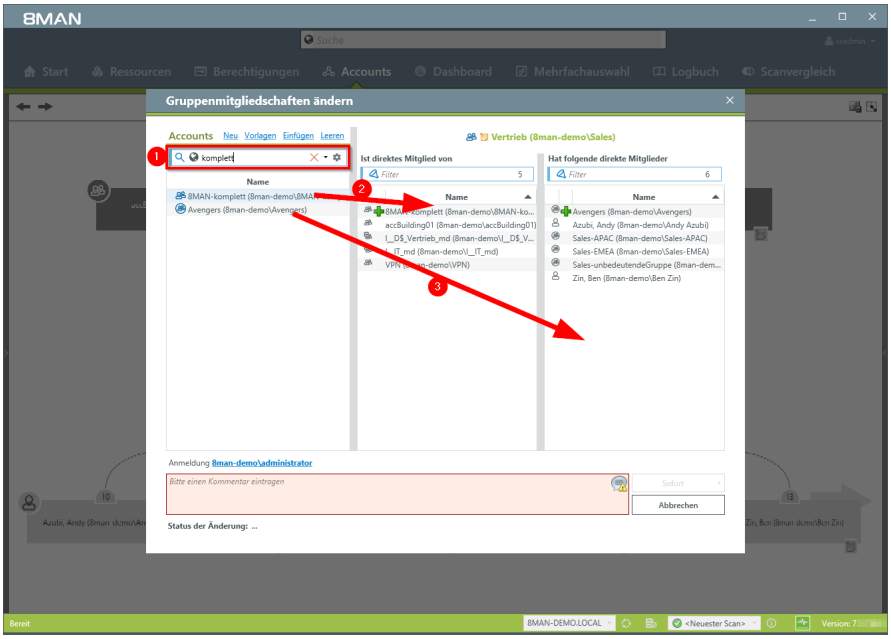
Gruppenmitgliedschaften im Bulk entfernen (Webclient)

Der Prozess in einzelnen Schritten

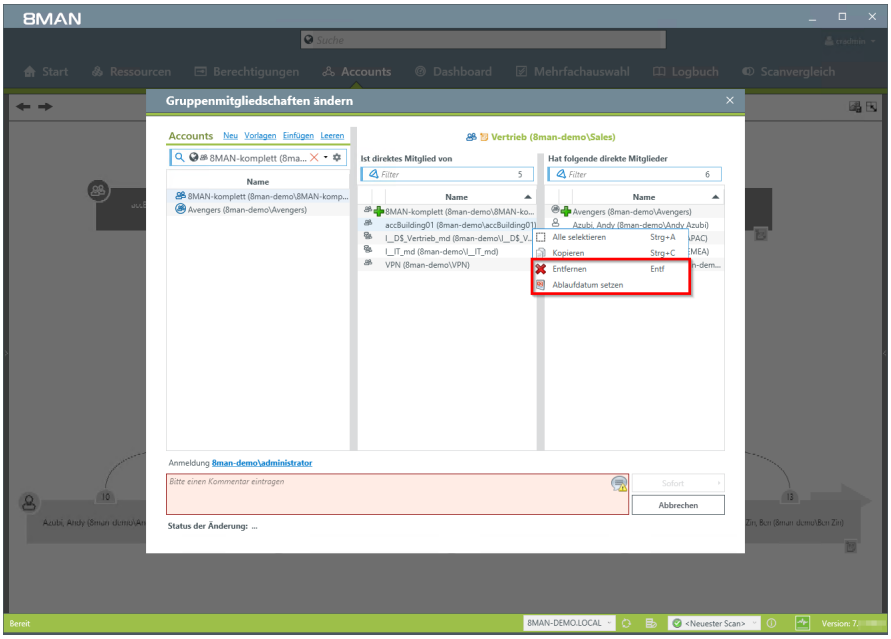


1. *Wählen Sie "Accounts".*
2. *Verwenden Sie die Suche, um das gewünschte Konto zu finden.*
3. *Rechtsklicken Sie das Konto und wählen "Ändern der Gruppenmitgliedschaften..." im Kontextmenü.*

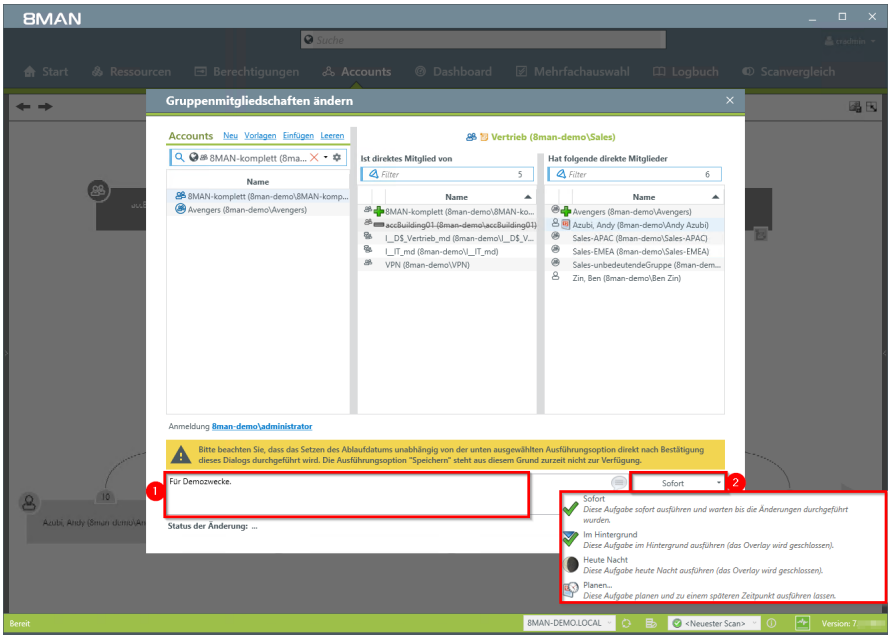
Alternativ können Sie auch "Gruppenmitgliedschaften bearbeiten" auf der Startseite aufrufen.



1. *Verwenden Sie die Suche, um Benutzer oder Gruppen zu finden.*
2. *Ziehen Sie eine Gruppe per Drag&Drop auf die mittlere Spalte, um eine neue Mitgliedschaft (Eltern) zu erzeugen.*
3. *Ziehen Sie den Benutzer oder die Gruppe per Drag&Drop auf die rechte Spalte, um der Gruppe neue Mitglieder (Kinder) hinzuzufügen.*



Benutzen Sie das Kontextmenü nach Rechtsklick, um Mitgliedschaften (Eltern und Kinder) sofort oder zu einem Ablaufdatum zu entfernen.



1. *Sie müssen einen Kommentar angeben.*
2. *Führen Sie die Änderungen sofort oder später aus.*

8.1.1.4 Leere Gruppen entfernen

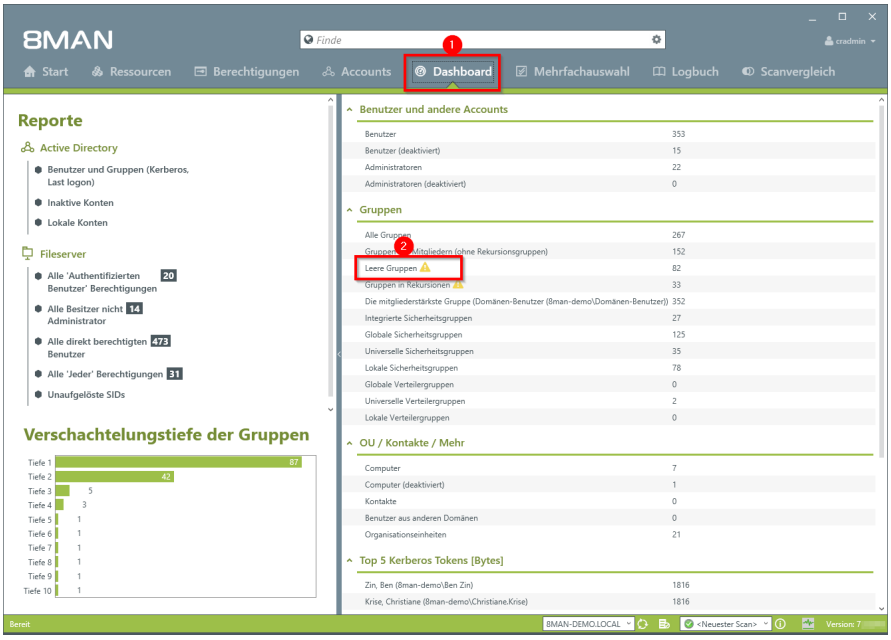
Hintergrund / Mehrwert

Im Active Directory sammeln sich über die Jahre leere Gruppen an. Diese verringern die Performance und behindern den Überblick. Wir empfehlen diese Gruppen zu löschen.

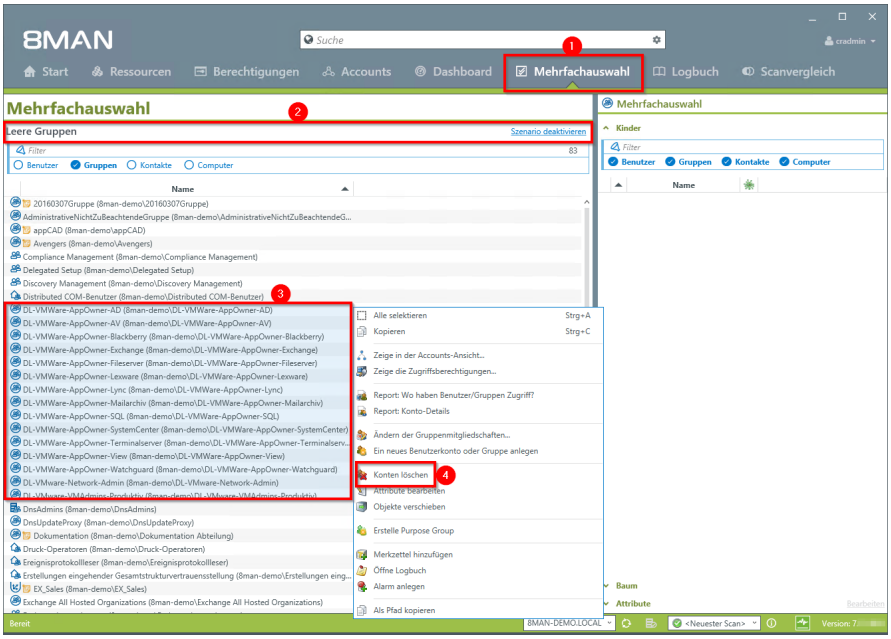
8MAN kann Nutzerkonten und Gruppen mit den dazugehörigen (Direkt-)Berechtigungseinträgen auf den Fileservern löschen. Dadurch ist das Sicherheitsrisiko der verwaisten SIDs obsolet.

Gruppen ohne Mitglieder können Systemgruppen sein. Diese sollten Sie nicht löschen.

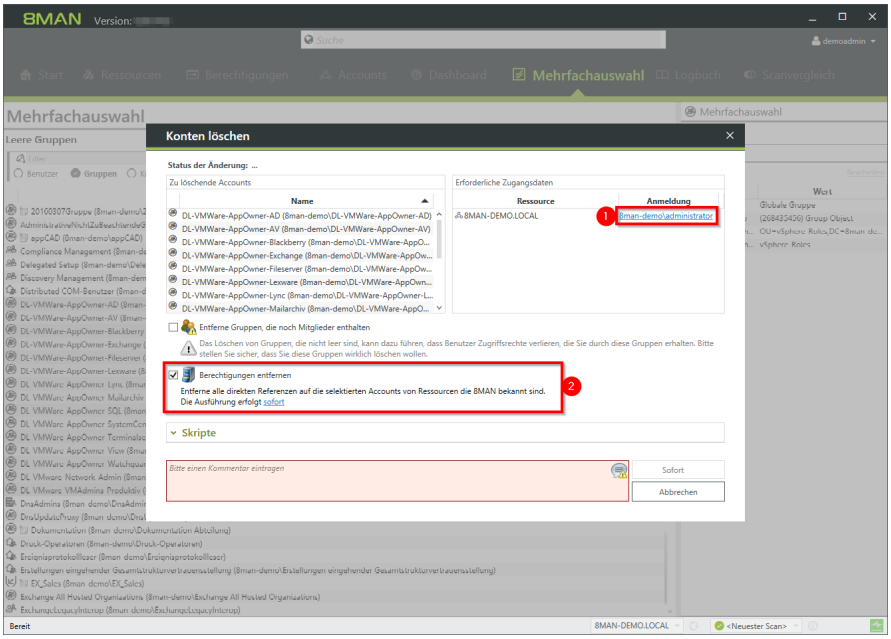
Der Prozess in einzelnen Schritten



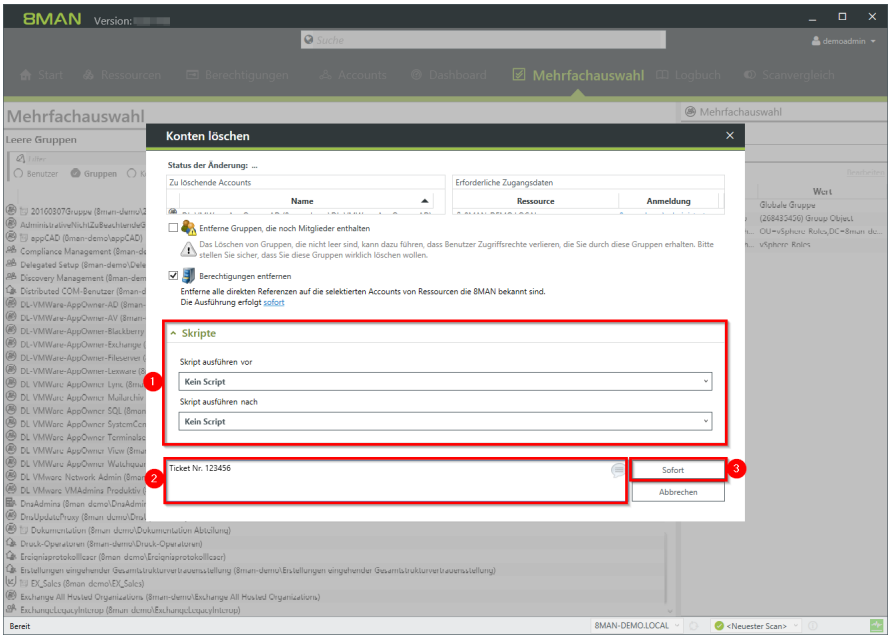
1. *Wählen Sie Dashboard.*
2. *Doppelklicken Sie auf "Leere Gruppen".*



1. *8MAN wechselt automatisch in die Mehrfachauswahl.*
2. *Das Szenario "Leere Gruppen" ist aktiv. Alle aufgelisteten Gruppen sind leer.*
3. *Markieren Sie die Gruppen, bei denen Sie sicher sind, dass sie gelöscht werden können.*
4. *Nach Rechtsklick wählen Sie im Kontextmenü "Konten löschen".*



1. *Optional: Ändern Sie die Anmeldung, mit der das Löschen der Gruppen im AD durchgeführt wird.*
2. *Aktivieren Sie die Option "Berechtigungen entfernen" und verhindern somit verwaiste SIDs.*



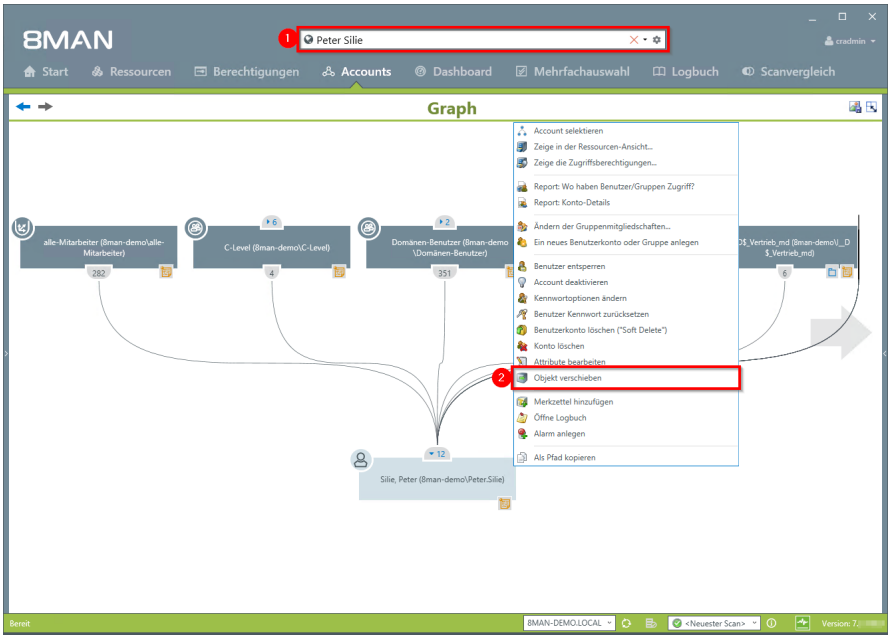
1. *Legen Sie fest, ob ein Skript vor oder nach dem Löschen ausgeführt werden soll. Siehe dazu: Skripte konfigurieren.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie den Löschvorgang.*

8.1.1.5 Objekte innerhalb des AD verschieben

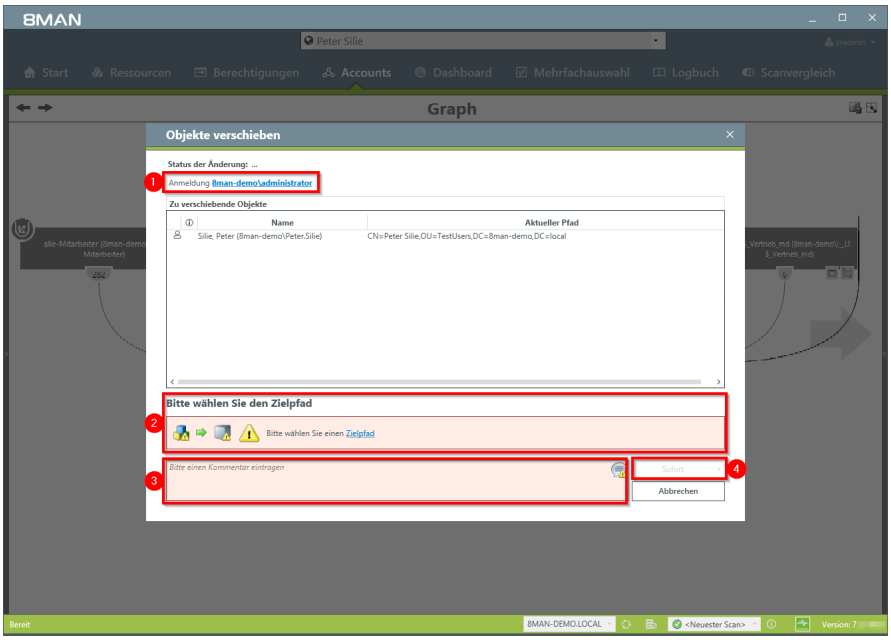
Hintergrund / Mehrwert

8MAN kann für Sie AD-Objekte, d. h. z. B. Nutzerkonten, Gruppen und Computer in andere OUs verschieben. Dies ist notwendig, wenn z. B. ein User den Standort wechselt und andere Gruppenrichtlinien für ihn gelten sollen. Mit 8MAN erfolgt das Verschieben dokumentiert und damit nachvollziehbar.

Der Prozess in einzelnen Schritten



1. *Finden Sie das gewünschte Objekt mit der Suche.*
2. *Rechtsklicken Sie das Objekt, z. B. in der Ansicht "Accounts", und wählen "Objekt verschieben".*



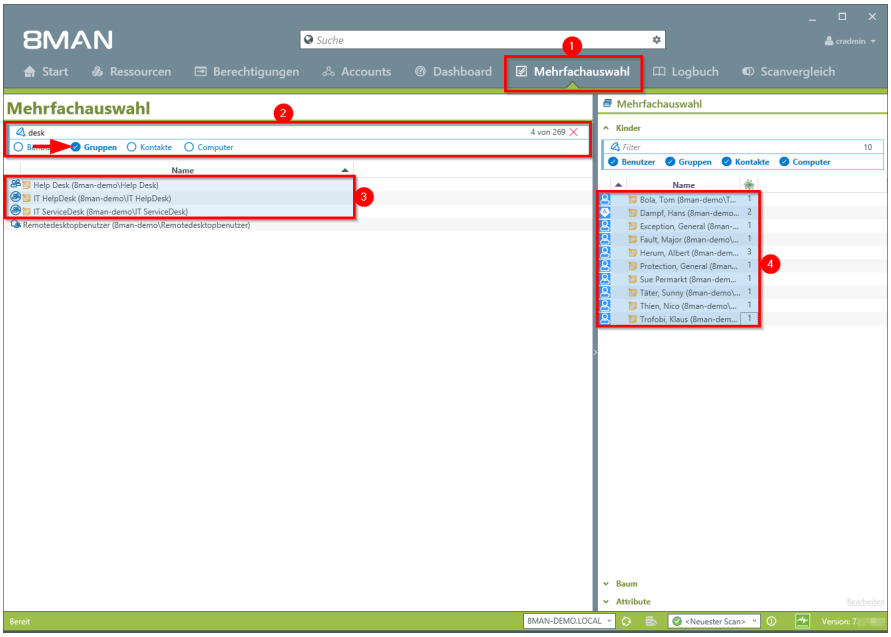
1. *Ändern Sie ggf. die Anmeldung, mit der das Verschieben ausgeführt werden soll.*
2. *Wählen Sie einen Zielpfad.*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie die Ausführung.*

8.1.1.6 Mehrere Gruppen auf eine Gruppe reduzieren

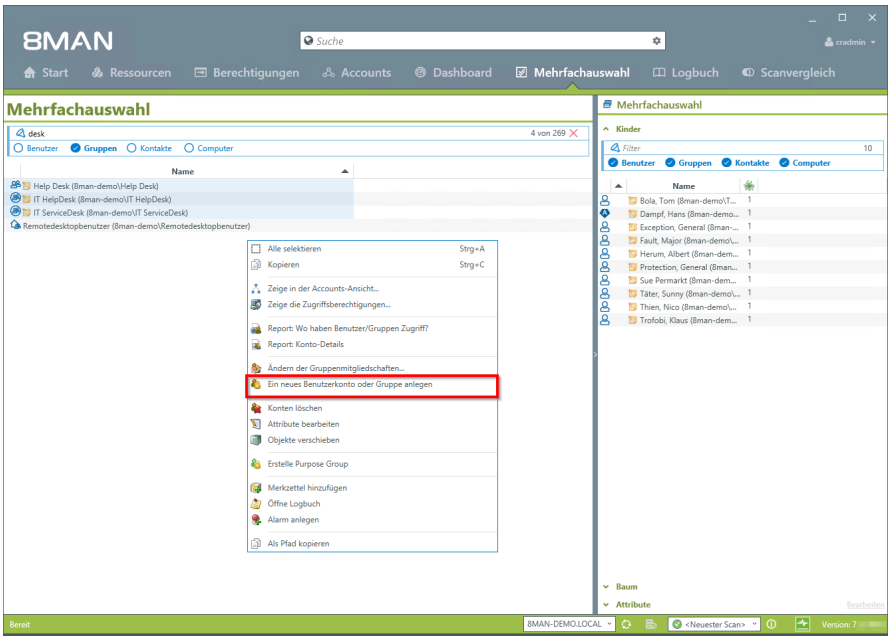
Hintergrund / Mehrwert

Ein übersichtliches AD verfügt über wenige Gruppen. Fassen Sie historisch gewachsene unnötige Gruppen zusammen. Im Beispiel wird eine zentrale Helpdesk-Gruppe erzeugt. Mit 8MAN können Sie die gewünschten Mitglieder einfach kopieren und dann in einer Gruppe zusammenfügen.

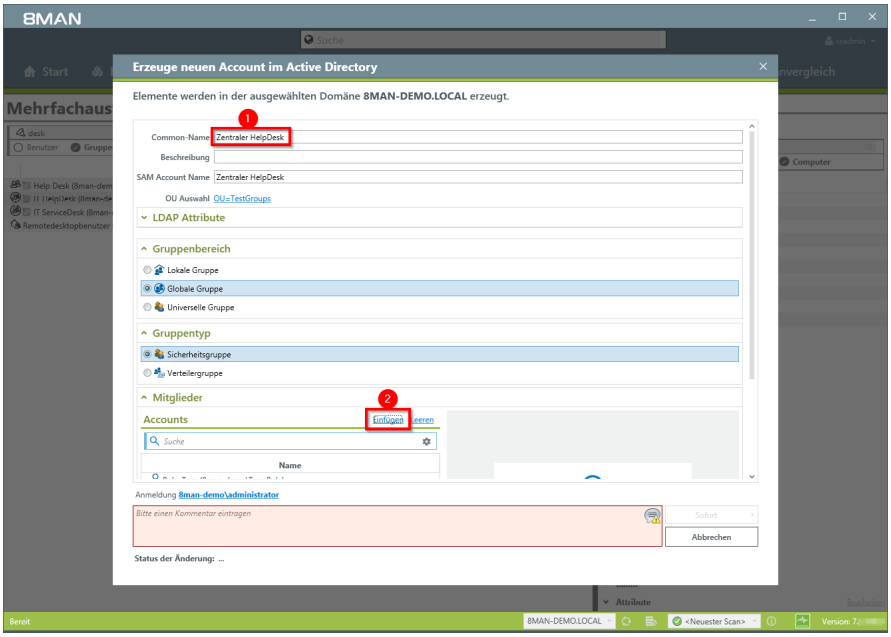
Der Prozess in einzelnen Schritten



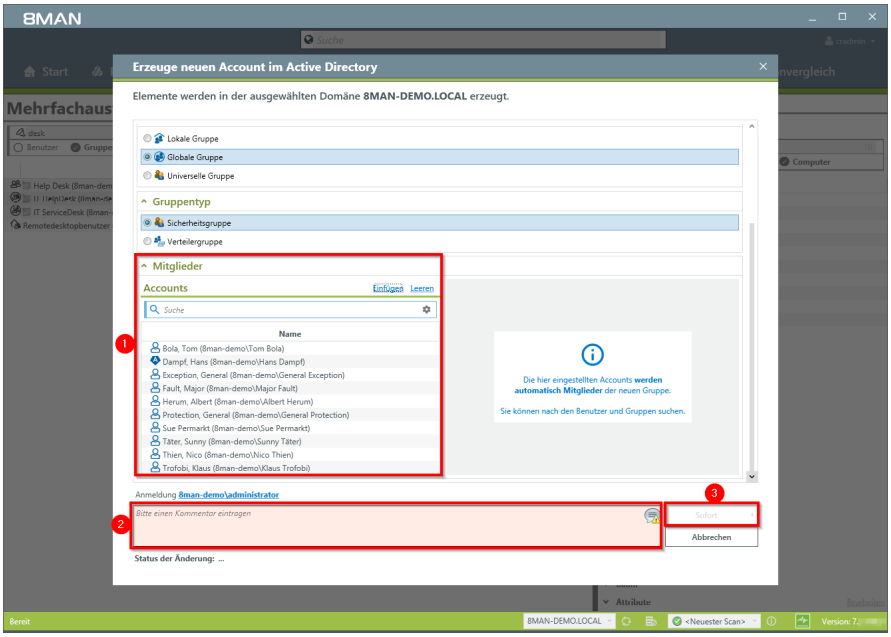
1. *Wählen Sie "Mehrfachauswahl".*
2. *Filtern Sie möglichst nach den gewünschten Gruppen.*
3. *Selektieren Sie die Gruppen.*
4. *Selektieren Sie alle Benutzer, z. B. mit der Tastenkombination "STRG"+"A". Kopieren Sie alle Benutzer in die Zwischenablage, z. B. mit der Tastenkombination "STRG"+"C".*



Rechtsklicken Sie und wählen Sie "Ein neues Benutzerkonto oder Gruppe anlegen".



1. *Geben Sie der neuen Gruppe einen Namen.*
2. *Klicken Sie im Bereich "Mitglieder" auf "Einfügen".*



1. *Alle Mitglieder der zuvor selektierten Gruppen sind in der neuen Gruppe "Zentraler HelpDesk".*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie die Erstellung der neuen Gruppe.*

8.1.1.7 Kennwortoptionen eines Benutzers ändern

Hintergrund / Mehrwert

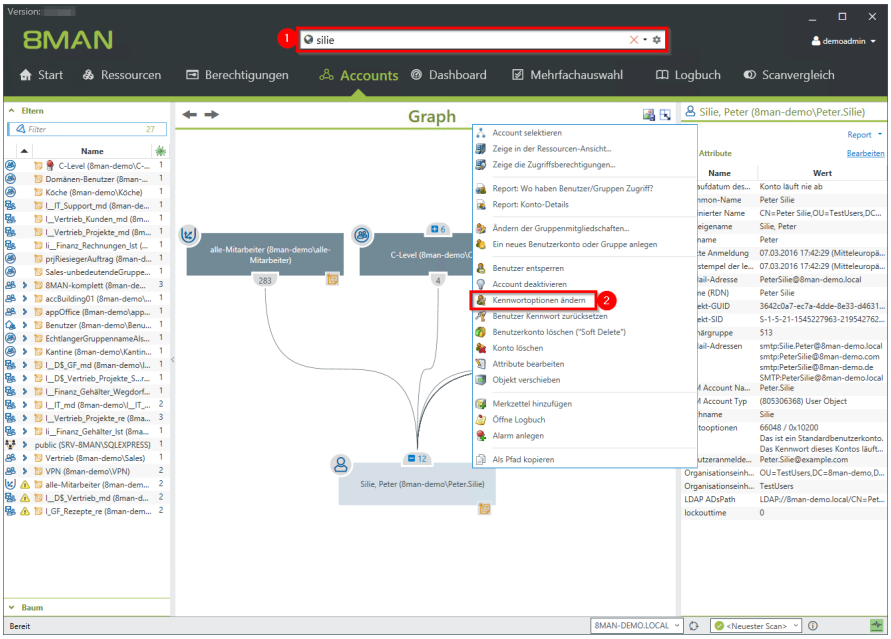
Kennwörter sollten regelmäßig geändert werden. Legen Sie die Kennwortoptionen für einen Benutzer fest.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.11 Regelung des Passwortgebrauchs, M 4.48 Passwortschutz unter Windows-Systemen sowie M 4.7 Änderung voreingestellter Passwörter.

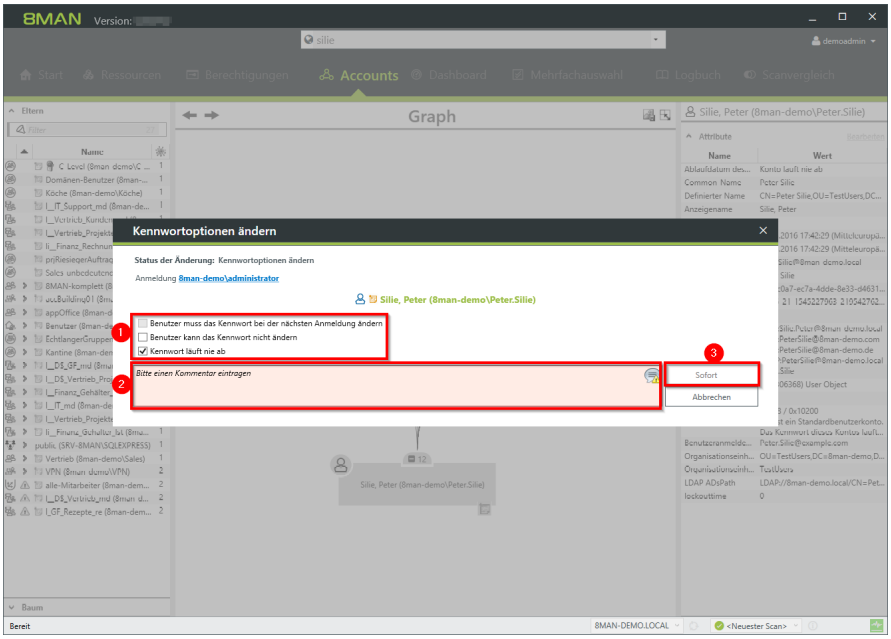
Weiterführende Services

Kennwortoptionen im Bulk ändern (Webclient).

Der Prozess in einzelnen Schritten



1. *Finden Sie den gewünschten Benutzer mit der Suche.*
2. *Rechtsklicken Sie den Benutzer, z. B. in der Accounts-Ansicht und wählen "Kennwortoptionen ändern" im Kontextmenü.*



1. *Legen Sie Kennwortoptionen fest.*
2. *Sie müssen einen Kommentar eingeben, z. B. "Ticketnummer", "Beauftragt von" oder "Genehmigt von".*
3. *Starten Sie die Ausführung.*

8.1.1.8 Konten im Bulk deaktivieren (Webclient)

Hintergrund / Mehrwert

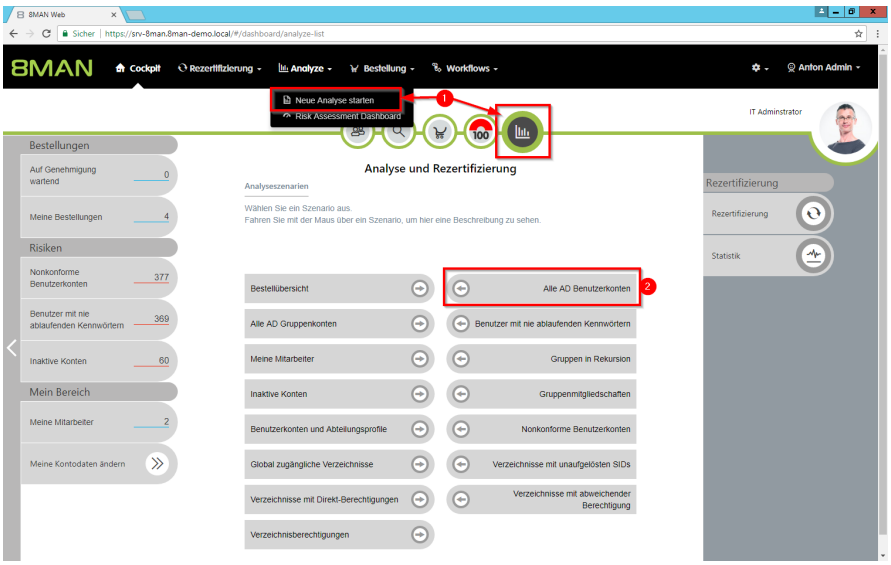
Nach einem Security Breach oder der Auflösung einer Abteilung macht es Sinn, mehrere Konten gleichzeitig zu deaktivieren. Erledigen Sie dies bequem im Webclient.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.

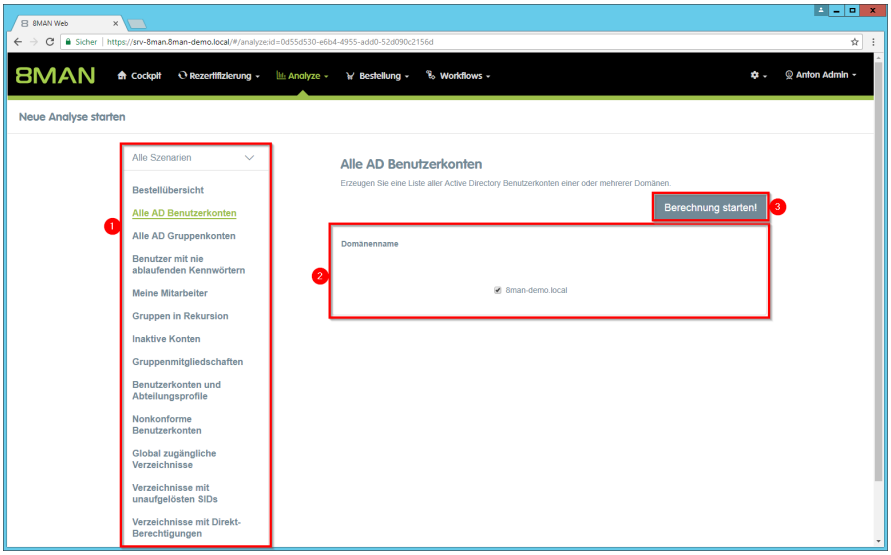
Weiterführende Services

Kennwort Optionen im Bulk ändern (Webclient)
Konten im Bulk löschen (soft delete) (Webclient)

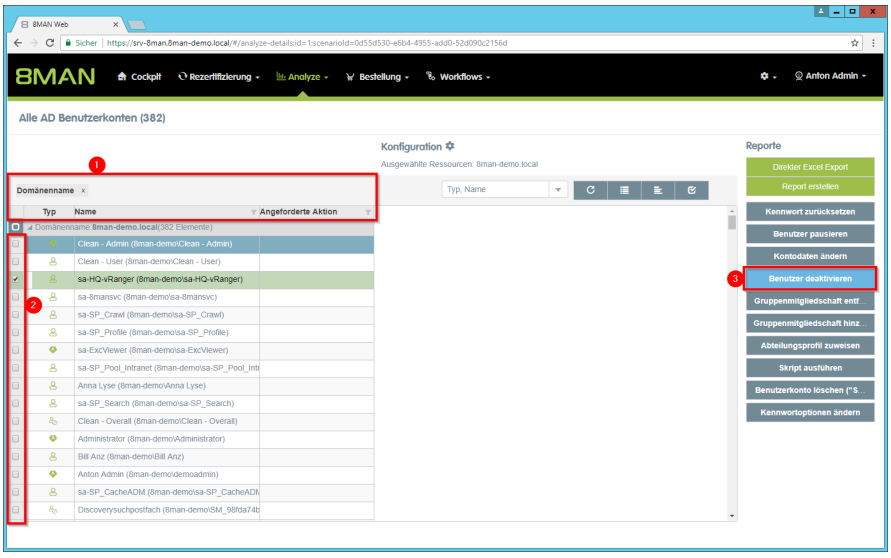
Der Prozess in einzelnen Schritten



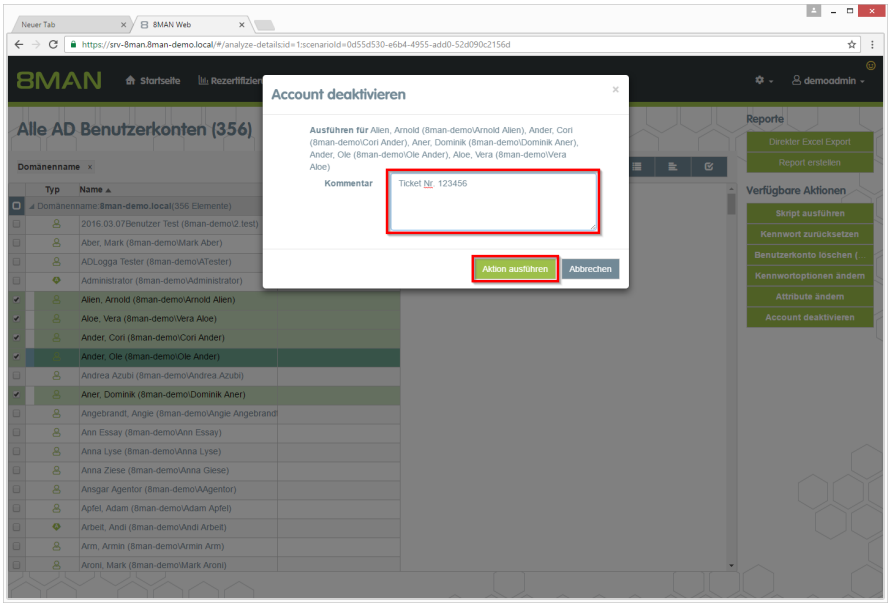
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Alle AD Benutzerkonten".*



1. *Optional: Wechseln Sie das Szenario.*
2. *Legen Sie Optionen für das Szenario fest.*
3. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
2. *Selektieren Sie die gewünschten Einträge.*
3. *Klicken Sie auf "Benutzer deaktivieren".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.1.9 Konten im Bulk löschen "soft delete" (Webclient)

Hintergrund / Mehrwert

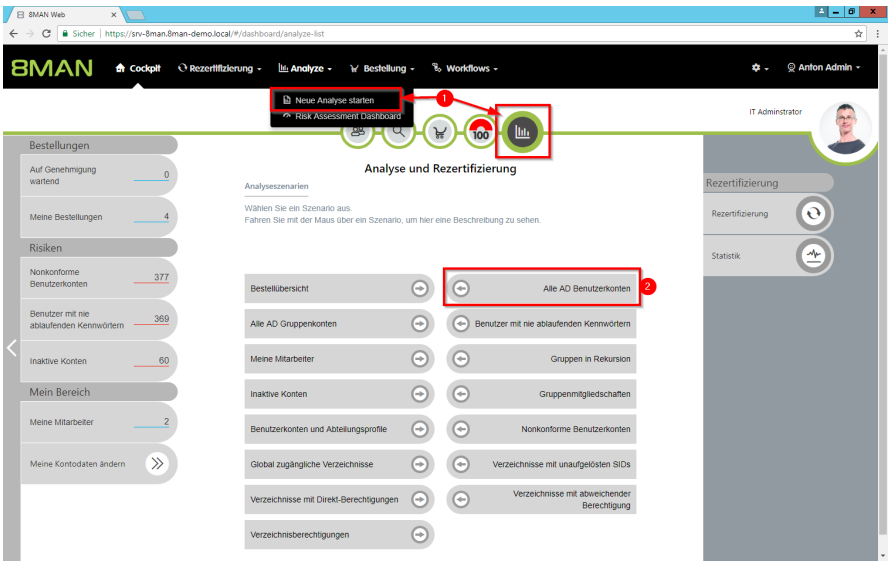
Nach einem Security Breach oder der Auflösung einer Abteilung macht es Sinn, mehrere Konten gleichzeitig zu löschen. Erledigen Sie dies bequem im Webclient.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.

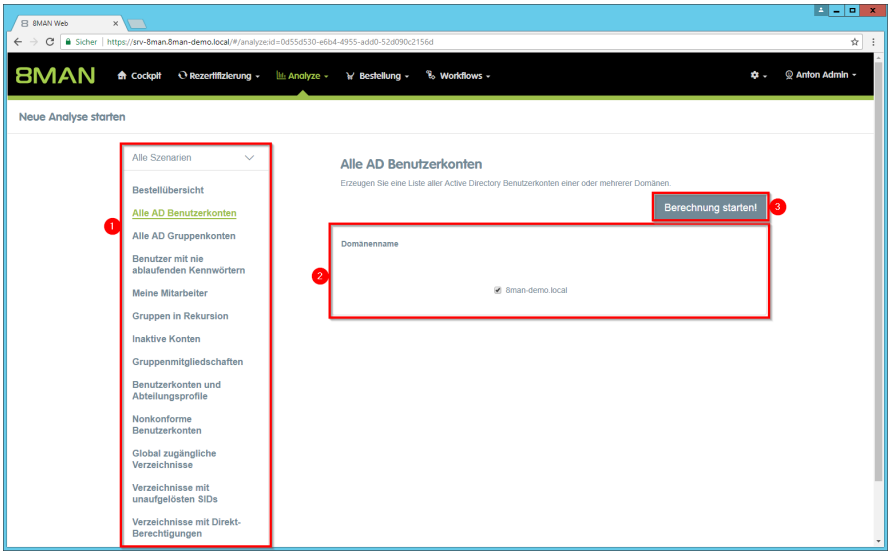
Weiterführende Services

Kennwort Optionen im Bulk ändern (Webclient)
Konten im Bulk löschen (soft delete) (Webclient)

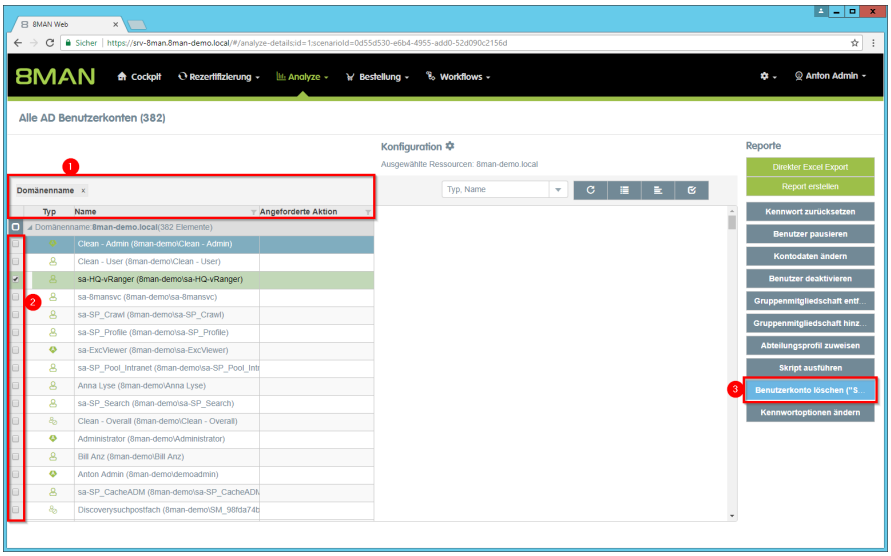
Der Prozess in einzelnen Schritten



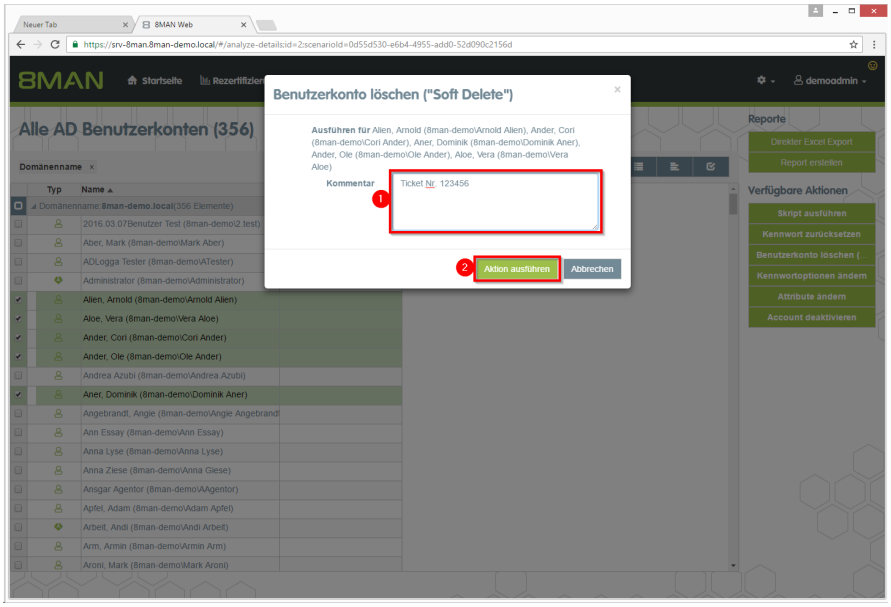
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Alle AD Benutzerkonten".*



1. *Optional: Wechseln Sie das Szenario.*
2. *Legen Sie Optionen für das Szenario fest.*
3. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
2. *Selektieren Sie die gewünschten Einträge.*
3. *Klicken Sie auf "Benutzerkonto löschen "Soft delete".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.1.10 Kennwortoptionen im Bulk ändern (Webclient)

Hintergrund / Mehrwert

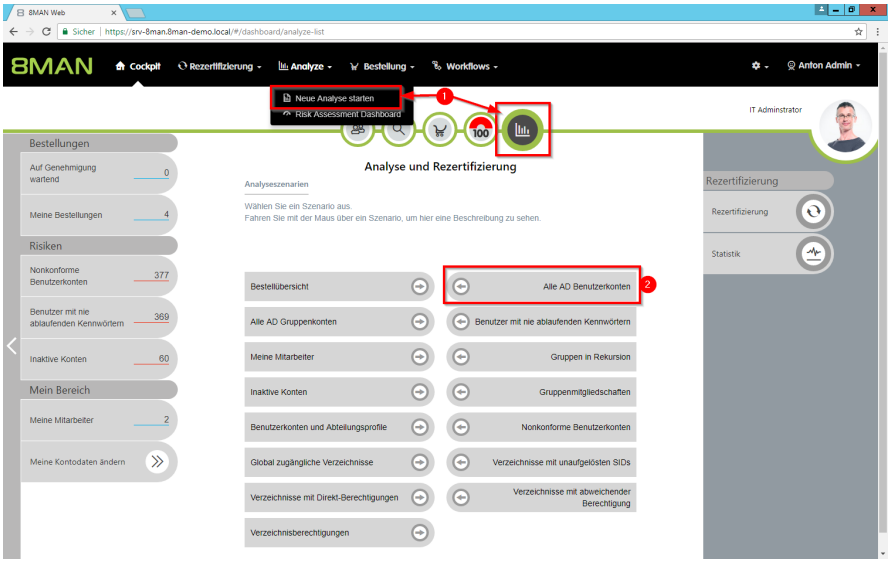
Kennwörter sollten regelmäßig geändert werden. Steuern Sie die Kennwortoptionen firmenweit und bequem über den Webclient.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.11 Regelung des Passwortgebrauchs, M 4.48 Passwortschutz unter Windows-Systemen sowie M 4.7 Änderung voreingestellter Passwörter.

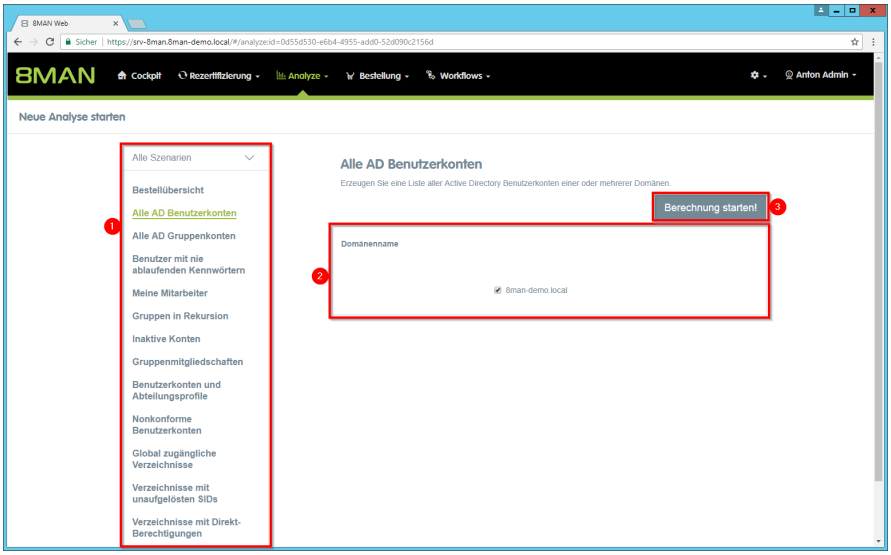
Ähnliche Services

Kennwörter im Bulk zurücksetzen (Webclient)

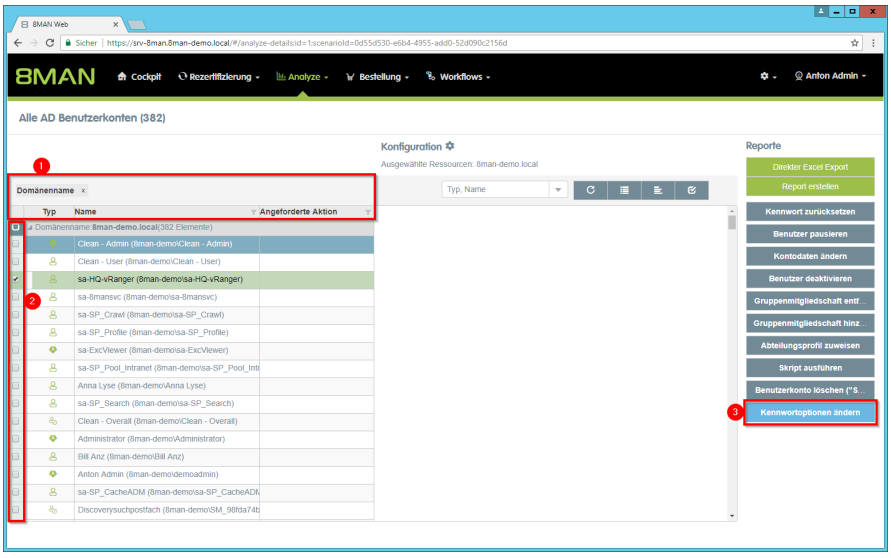
Der Prozess in einzelnen Schritten



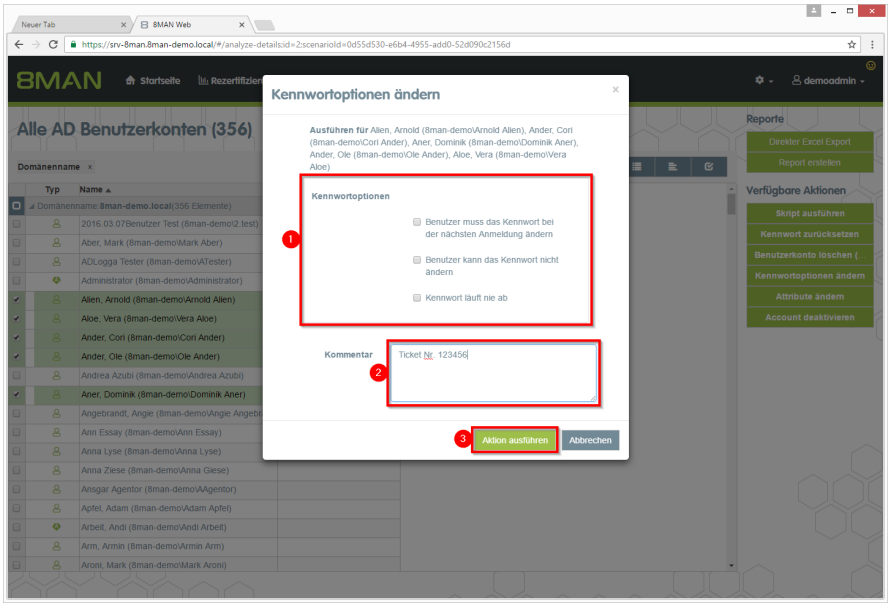
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Alle AD Benutzerkonten".*



1. *Optional: Wechseln Sie das Szenario.*
2. *Legen Sie Optionen für das Szenario fest.*
3. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
2. *Selektieren Sie die gewünschten Einträge.*
3. *Klicken Sie auf "Kennwortoptionen ändern".*



1. *Setzen Sie die Kennwortoptionen.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.1.11 Attribute im Bulk ändern (Webclient)

Hintergrund / Mehrwert

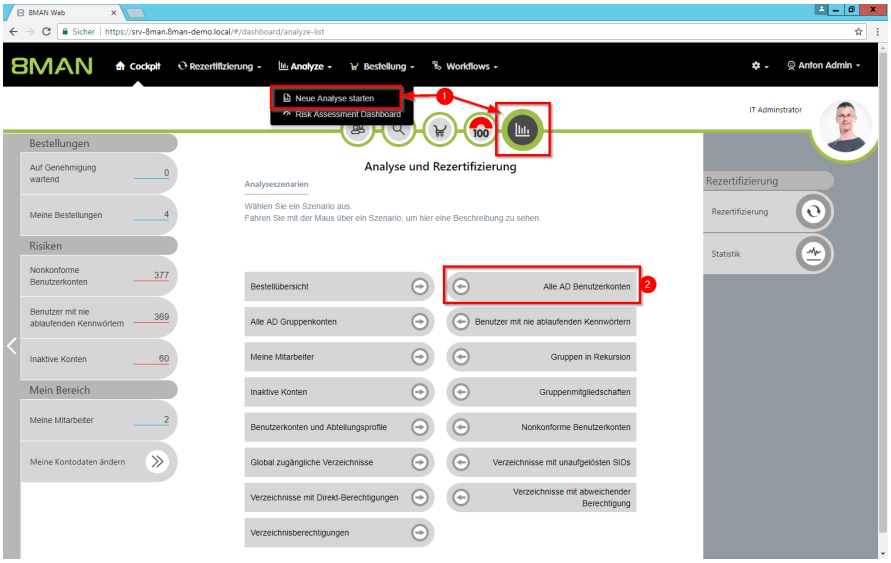
Mit 8MAN können Sie auch AD Attribute im Bulk ändern. Dies wird z.B. im Hinblick auf Kontaktdaten nach einem Firmen- oder Geschäftsstellenumzug relevant.

8MAN bietet ein Standardset von änderbaren Attributen. Sie können pro 8MAN-Rolle festlegen, welche Attribute angezeigt werden und damit änderbar sind. Bitte wenden Sie sich in solchen Fällen an unseren Support.

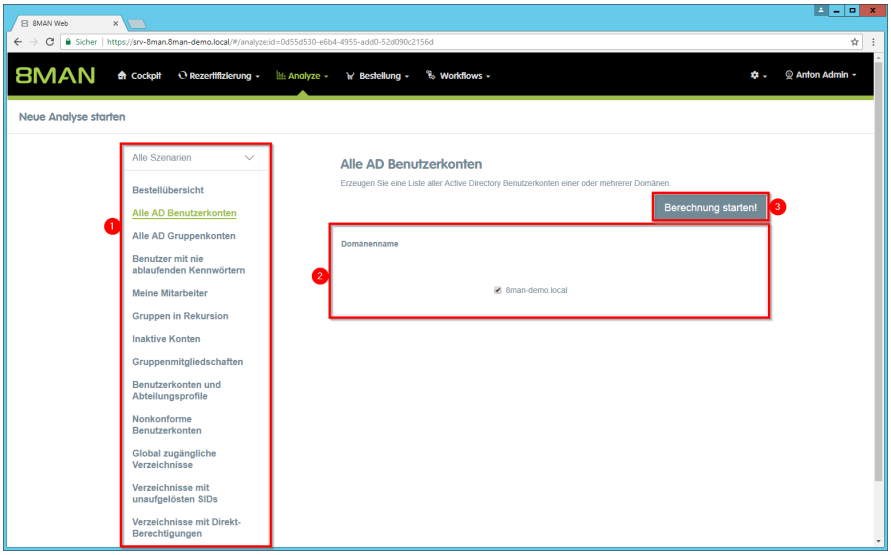
Weiterführende Services

Kennwort Optionen im Bulk ändern (Webclient)
Scripte für Nutzerkonten im Bulk ausführen (Webclient)

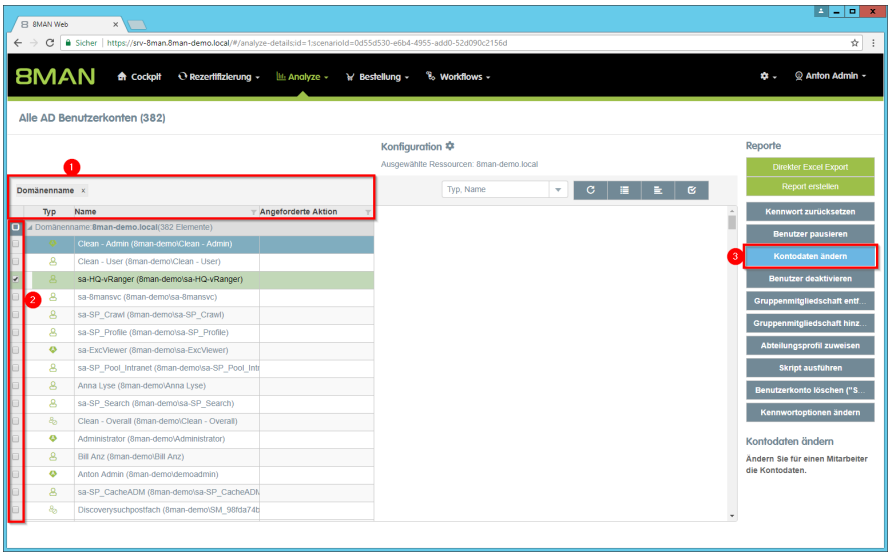
Der Prozess in einzelnen Schritten



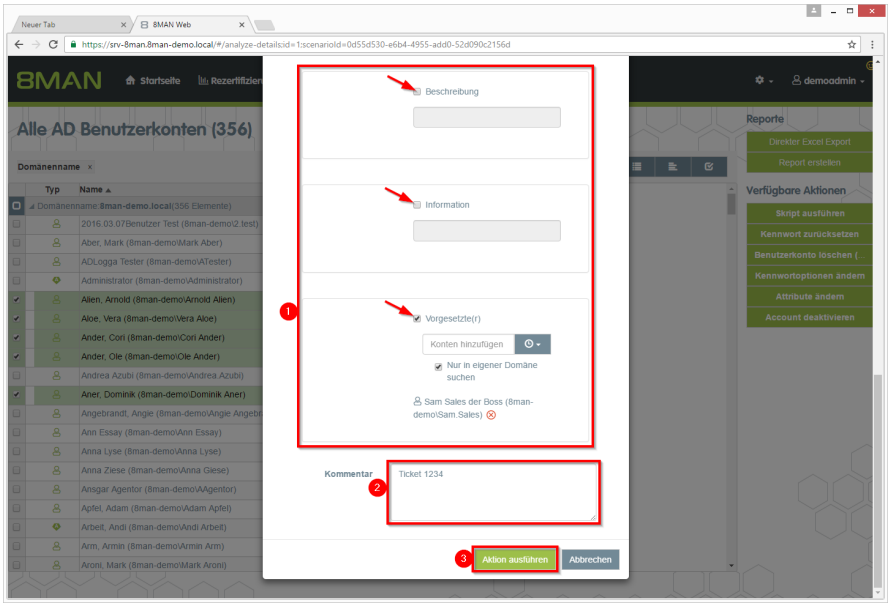
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Alle AD Benutzerkonten".*



1. *Optional: Wechseln Sie das Szenario.*
2. *Legen Sie Optionen für das Szenario fest.*
3. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
2. *Selektieren Sie die gewünschten Einträge.*
3. *Klicken Sie auf "Attribute ändern".*



1. *Aktivieren Sie die Attribute, die geändert werden sollen und tragen die Werte ein.*

Geben Sie keinen Wert an, werden die Inhalte der Attribute gelöscht.

2. *Sie müssen einen Kommentar eingeben.*
3. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort

ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

Die in dem Dialog angezeigten Attribute können pro Rolle angepasst werden. Dazu muss eine Anpassung der Konfigurationsdatei vorgenommen werden. Eine Anleitung finden Sie in unserer Knowledgebase (Login erforderlich).

8.1.1.12 Verwaiste SIDs im Bulk löschen (Webclient)

Hintergrund / Mehrwert

SIDs (Security Identifier) sind Zeichenfolgen, die einen Benutzer oder eine Gruppe eindeutig identifizieren. Werden direkt berechtigte Benutzer oder Gruppen im AD gelöscht, bleiben verwaiste SIDs im Dateisystem bestehen. Verwaiste SIDs ermöglichen eine Manipulation des Security-Tokens. Mit Hilfe der verwaisten SID können Innentäter sich Zugriff auf Ressourcen verschaffen.

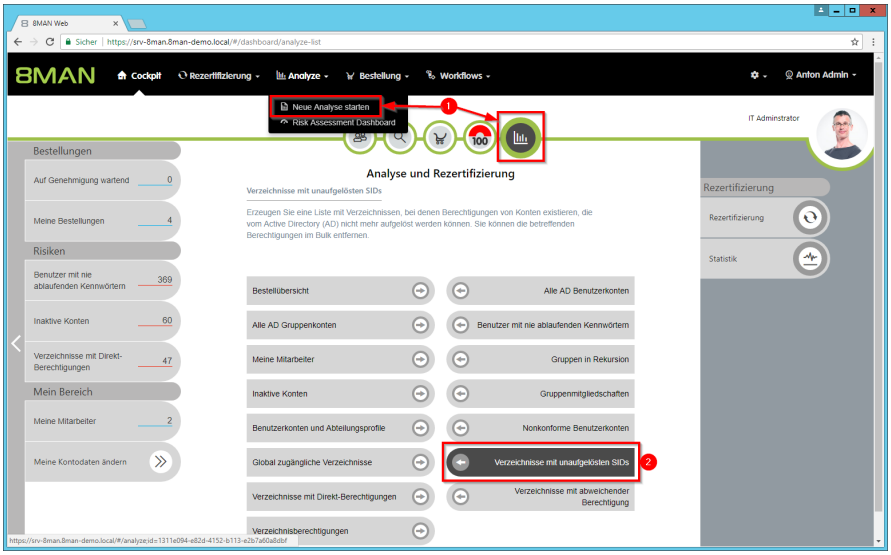
Mit dem 8MATE Analyze und Act löschen Sie verwaiste SIDs im Bulk.

Weiterführende Services

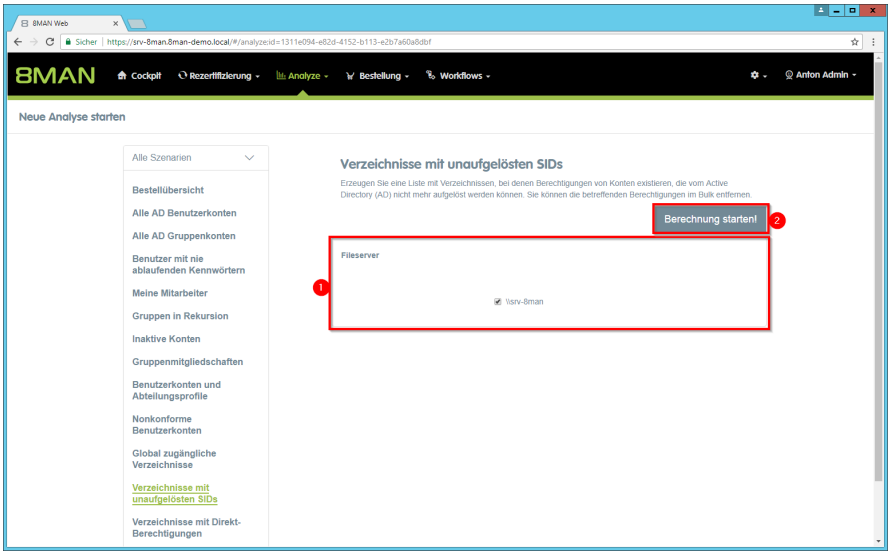
Verwaiste SIDs identifizieren und löschen (einzeln im Rich Client)

Report: Verwaiste SIDs identifizieren (im Rich Client)

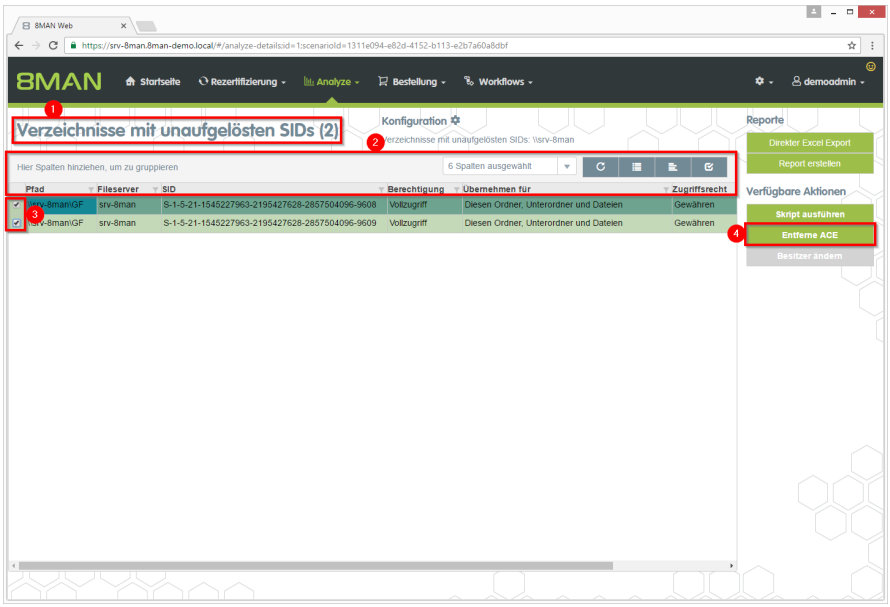
Der Prozess in einzelnen Schritten



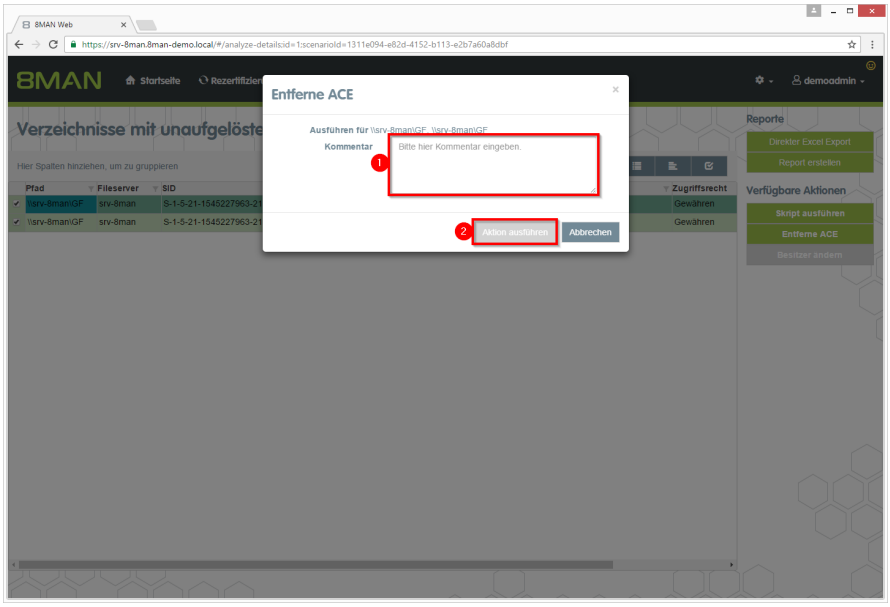
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Verzeichnisse mit unaufgelösten SIDs".*



1. *Wählen Sie die Fileserver aus.*
2. *Klicken Sie auf "Berechnung starten".*



1. *8MAN zeigt Ihnen eine Auflistung aller unaufgelösten SIDs.*
2. *Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
3. *Selektieren Sie die gewünschten Einträge.*
4. *Klicken Sie auf "Entferne ACE".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.1.13 Direktberechtigungen im Bulk entfernen (Webclient)

Hintergrund / Mehrwert

Direktberechtigungen sollten unter allen Umständen vermieden werden und durch Berechtigungen über Gruppen ersetzt werden. Direktberechtigungen sind ineffizient, weil jeder Nutzer einzeln berechtigt werden muss. Darüber hinaus müssen Sie alle Verzeichnisse bei der Rechteentfernung berücksichtigen.

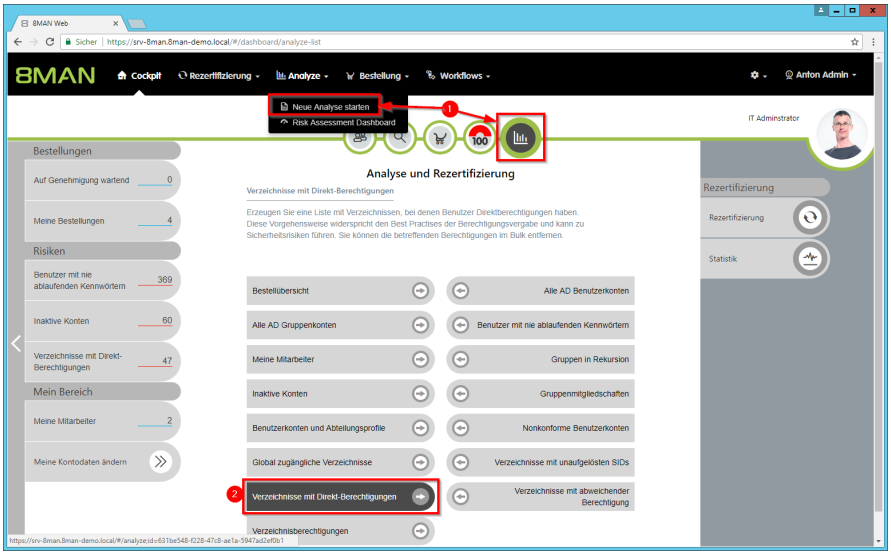
Im Webclient entfernen Sie Direktberechtigungen im Bulk.

Weiterführende Services

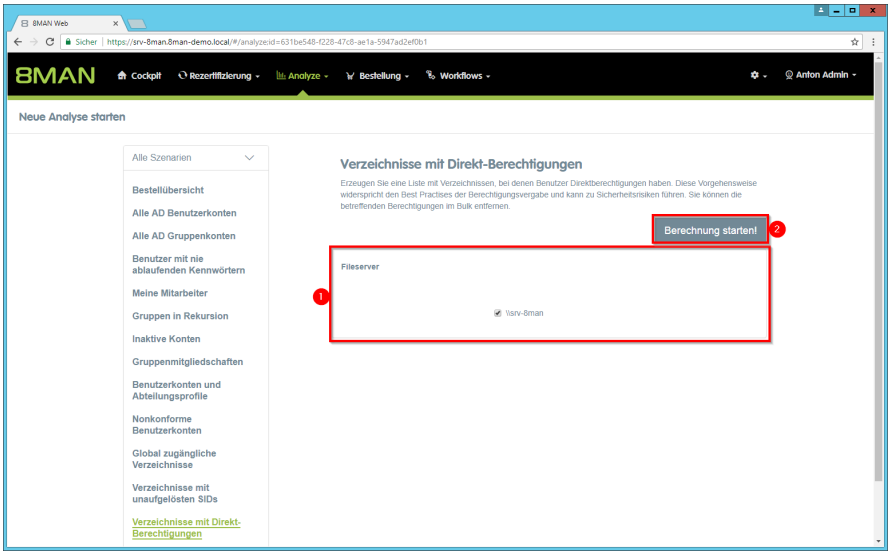
Verwaiste SIDs im Bulk löschen (Webclient)

Direktberechtigungen entfernen (einzeln im Rich Client)

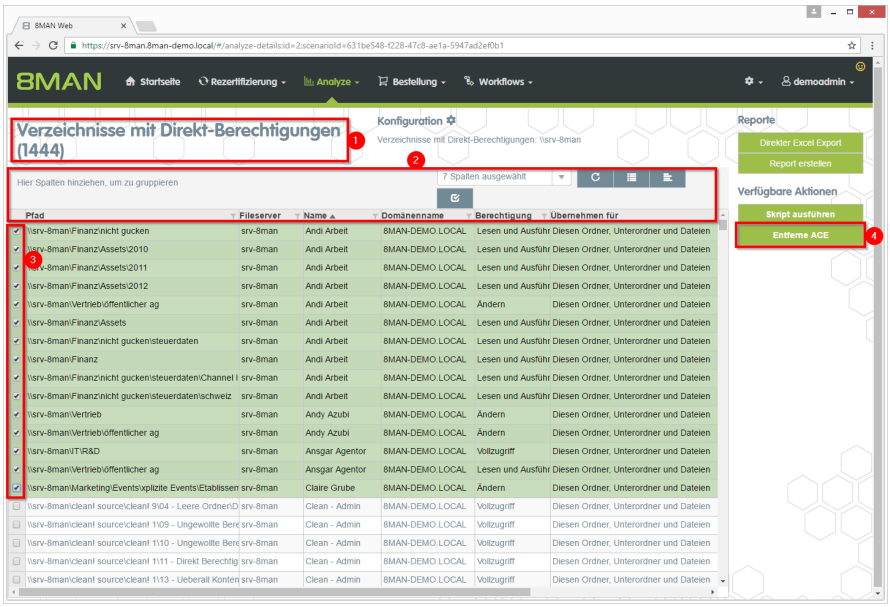
Der Prozess in einzelnen Schritten



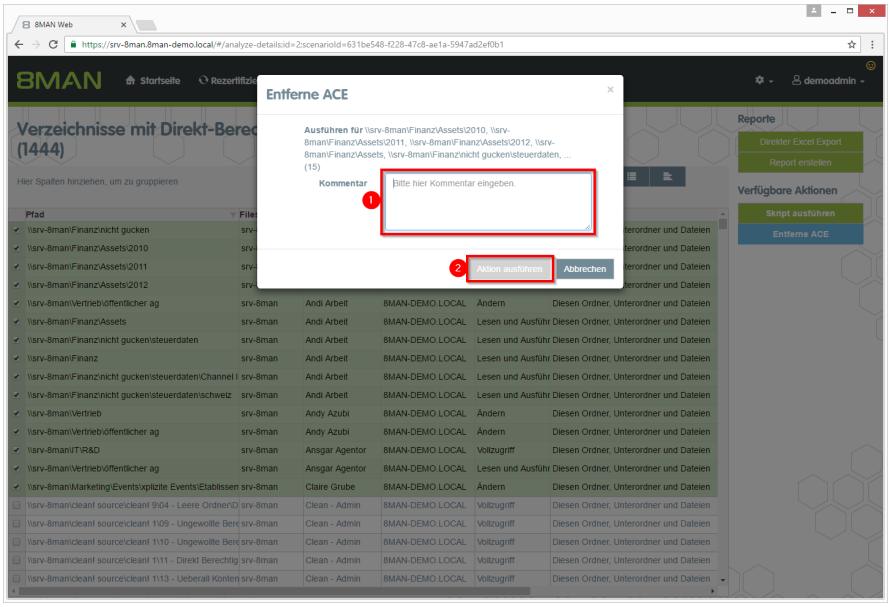
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Verzeichnisse mit Direktberechtigungen".*



1. *Wählen Sie die Fileserver aus.*
2. *Klicken Sie auf "Berechnung starten".*



1. *8MAN zeigt Ihnen eine Auflistung aller Verzeichnisse mit Direktberechtigungen.*
2. *Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
3. *Selektieren Sie die gewünschten Einträge.*
4. *Klicken Sie auf "Entferne ACE".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.1.14 Gruppenmitgliedschaften im Bulk entfernen (Webclient)

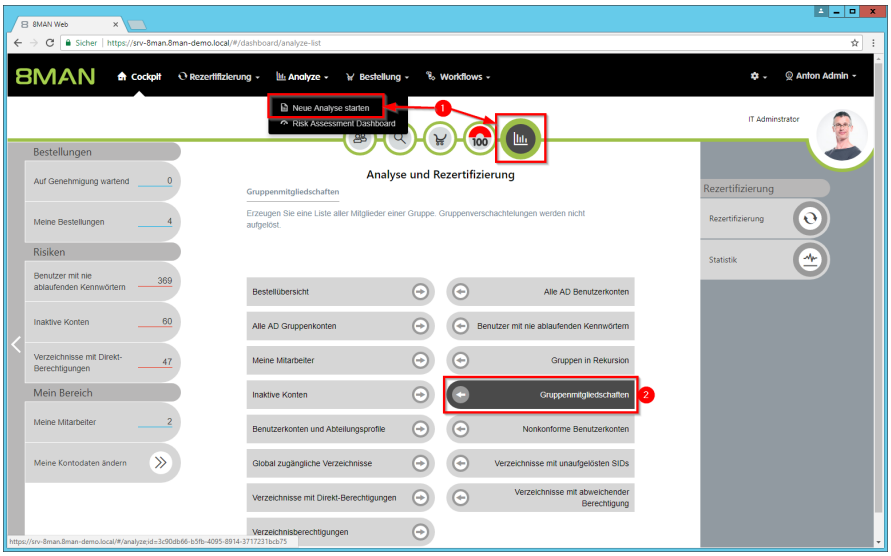
Hintergrund / Mehrwert

Mit Analyze & Act können Sie schnell Gruppenmitgliedschaften entfernen.

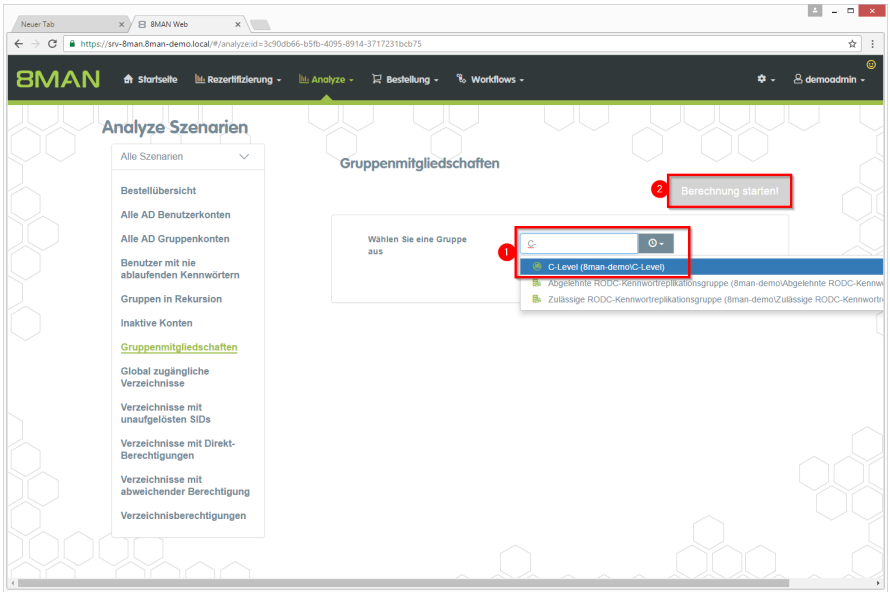
Weiterführende Services

Gruppenmitgliedschaften bearbeiten (Rich Client)

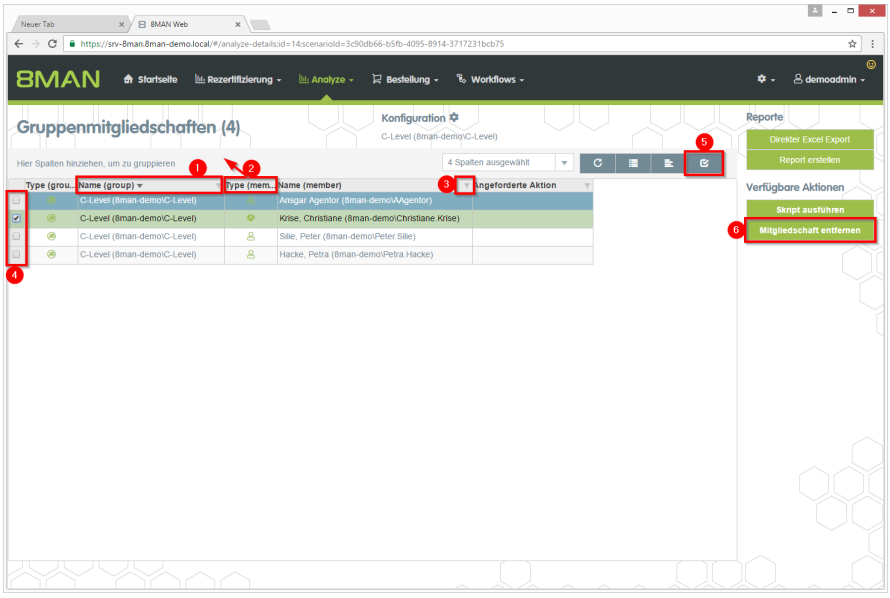
Der Prozess in einzelnen Schritten



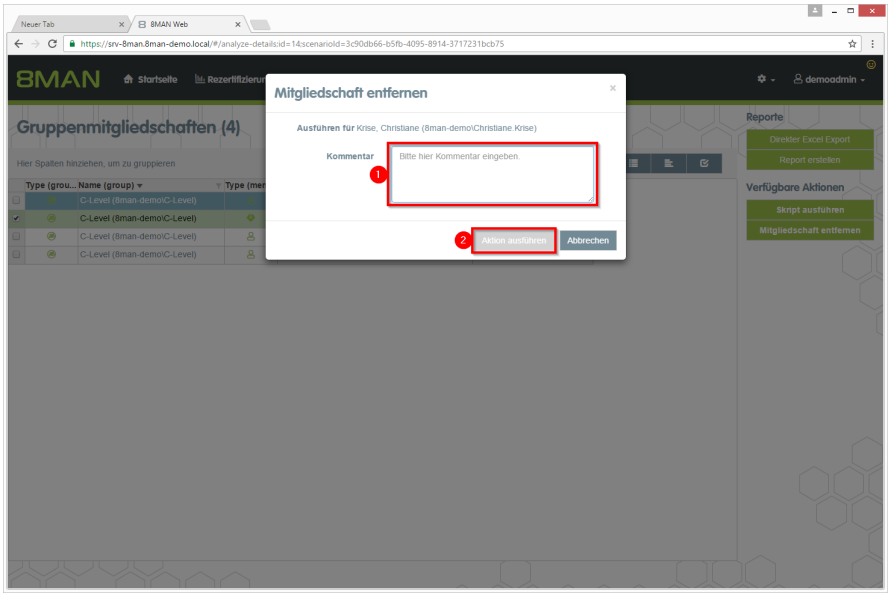
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Gruppenmitgliedschaften".*



1. *Wählen Sie eine Gruppe.*
2. *Klicken Sie auf "Berechnung starten".*



1. *Zum Sortieren klicken Sie auf einen Spaltenkopf.*
2. *Zum Gruppieren ziehen Sie einen Spaltenkopf nach oben.*
3. *Zum Filtern klicken Sie auf das Filtersysmbol.*
4. *Selektieren sie gewünschte Einträge.*
5. *Selektieren Sie alle Einträge.*
6. *Klicken Sie auf "Mitgliedschaft entfernen".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.1.15 "Jeder" Berechtigungen im Bulk entfernen (Webclient)

Hintergrund / Mehrwert

Werden "Jeder-Konten" für die Vergabe von Berechtigungen benutzt, hat (fast) jeder Zugriff auf verknüpften Ressourcen. Die Folge ist eine massive Überberechtigung, also eine hohe Chance für unberechtigte Zugriffe.

Zu den "Jeder-Konten" gehören:

- Jeder
- Authentifizierte Benutzer
- Domänen-Benutzer

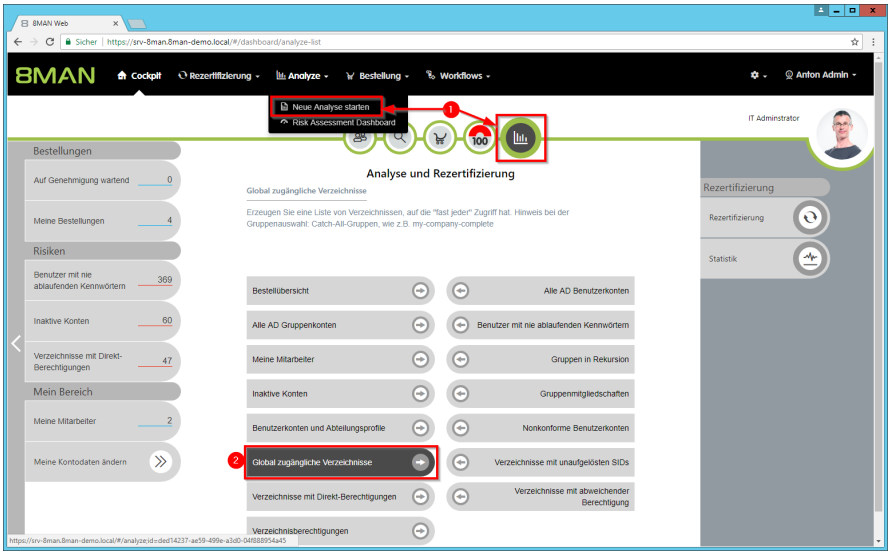
Bevor Sie die Berechtigungen löschen, sollten Sie, falls noch nicht vorhanden, den Ressourcen spezifische Gruppen zuweisen.

Weiterführende Services

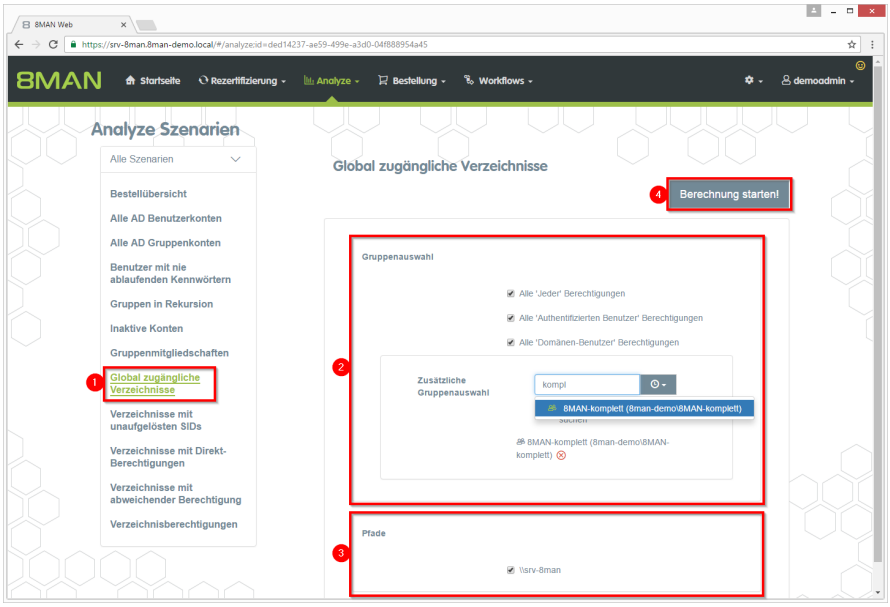
Report: Jeder Berechtigungen (Rich Client)

Report: Authentifizierte Benutzer Berechtigungen (Rich Client)

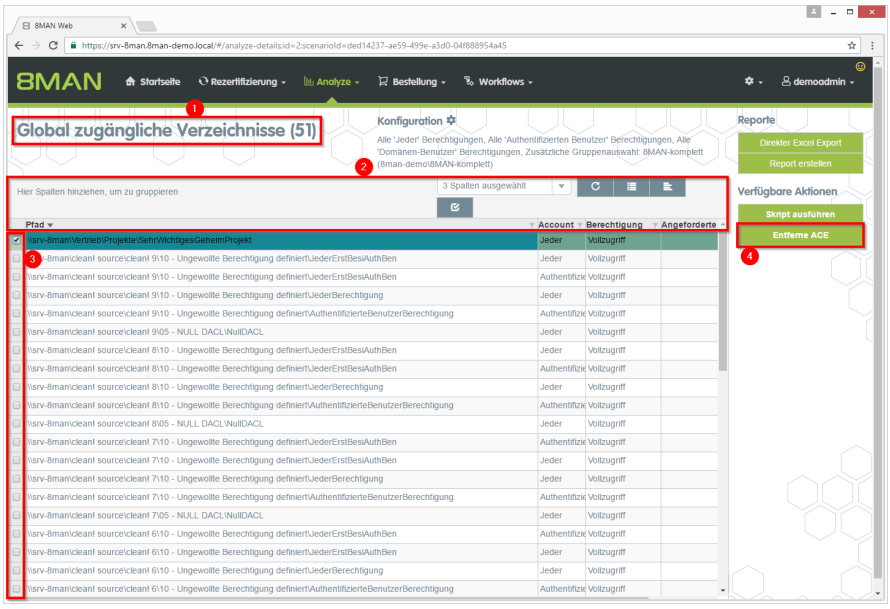
Der Prozess in einzelnen Schritten



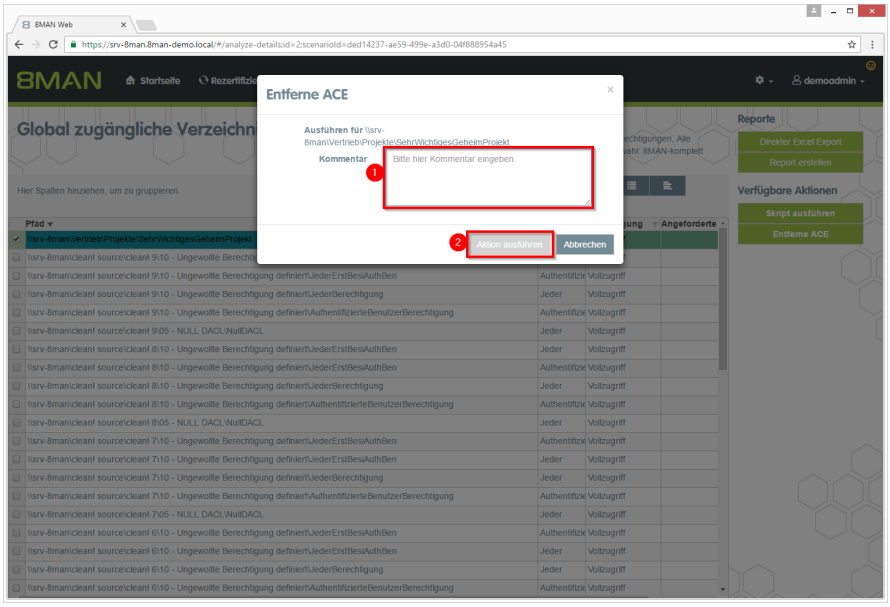
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Global zugängliche Verzeichnisse".*



1. *Klicken Sie auf "Global zugängliche Verzeichnisse".*
2. *Wählen Sie die Gruppen aus. Sie können eine zusätzliche Gruppe hinzufügen. Diese Option eignet sich besonders für sogenannte "catch-all" Gruppen, z.B. "meineFirma-komplett".*
3. *Wählen Sie die Fileserver aus.*
4. *Klicken Sie auf "Berechnung starten".*



1. *8MAN zeigt Ihnen eine Auflistung aller global zugänglichen Verzeichnisse.*
2. *Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
3. *Selektieren Sie die gewünschten Einträge.*
4. *Klicken Sie auf "Entferne ACE".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.1.16 Ein neues Abteilungsprofil erstellen (Webclient)

Hintergrund / Mehrwert

8MAN setzt im Bereich User Provisioning neue Maßstäbe: Mit der Einführung von Abteilungsprofilen definieren Abteilungsleiter zusammen mit der Geschäftsführung und dem Compliance Officer den Handlungsradius von Mitarbeitern im Unternehmen.

Mit der Entwicklung abteilungsspezifischer Profile werden somit De-Facto Standards gesetzt, mit deren Implementierung Sie den gesamten Joiner-Mover-Leaver Prozess optimieren:

Abteilungsprofile können Attribute und Gruppenmitgliedschaften enthalten.

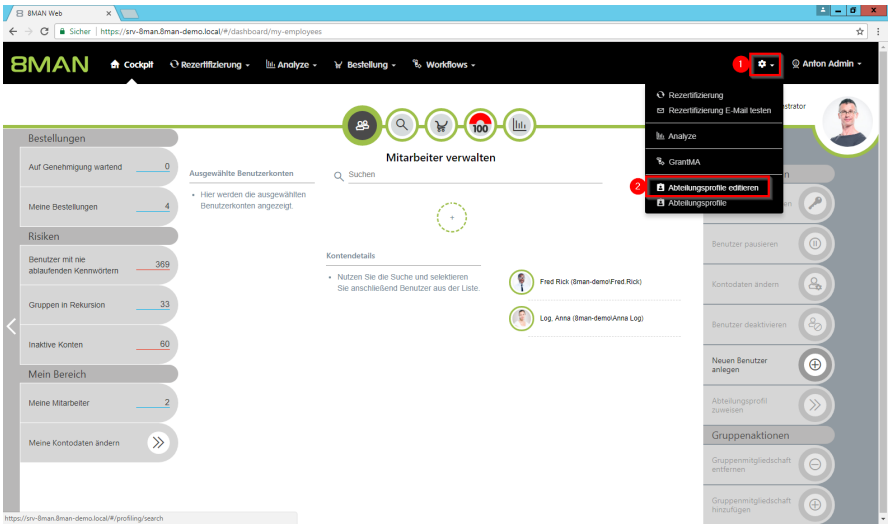
Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle sowie M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements.

Weiterführende Services

Benutzern ein Abteilungsprofil zuweisen (Webclient)

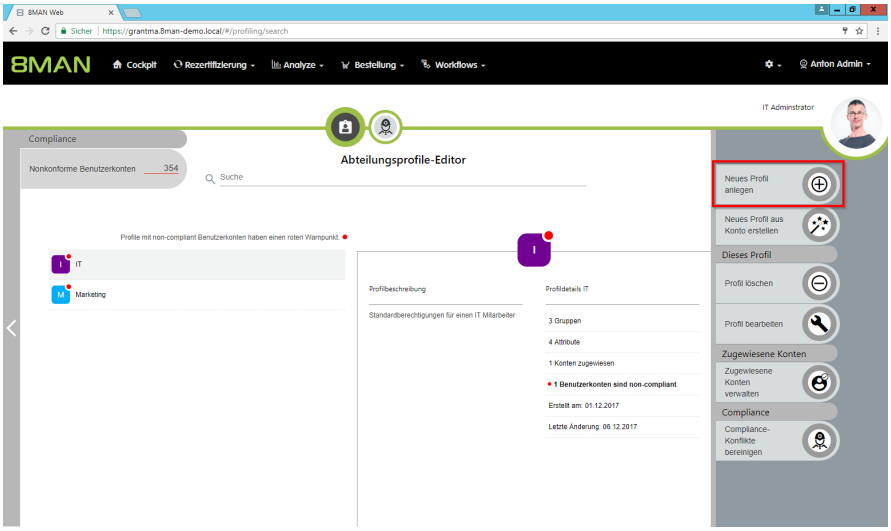
Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check) (Webclient)

Der Prozess in einzelnen Schritten

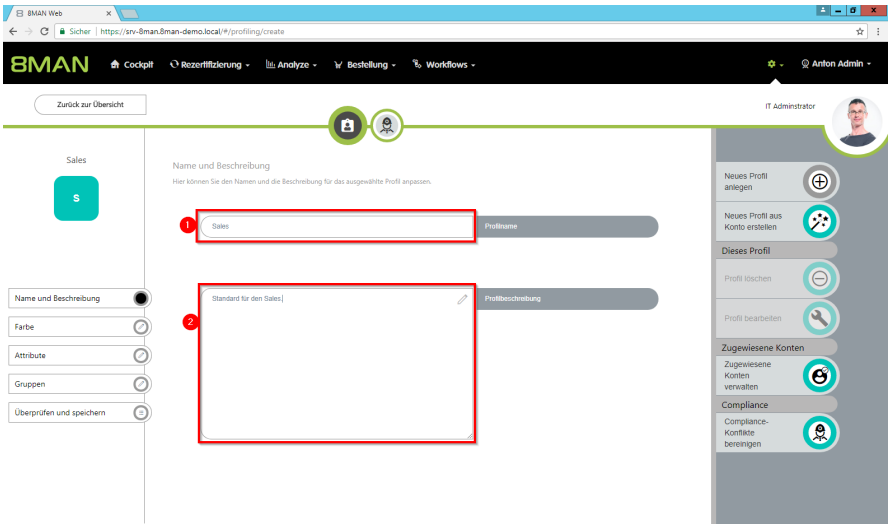


Klicken Sie auf "Abteilungsprofile editieren".

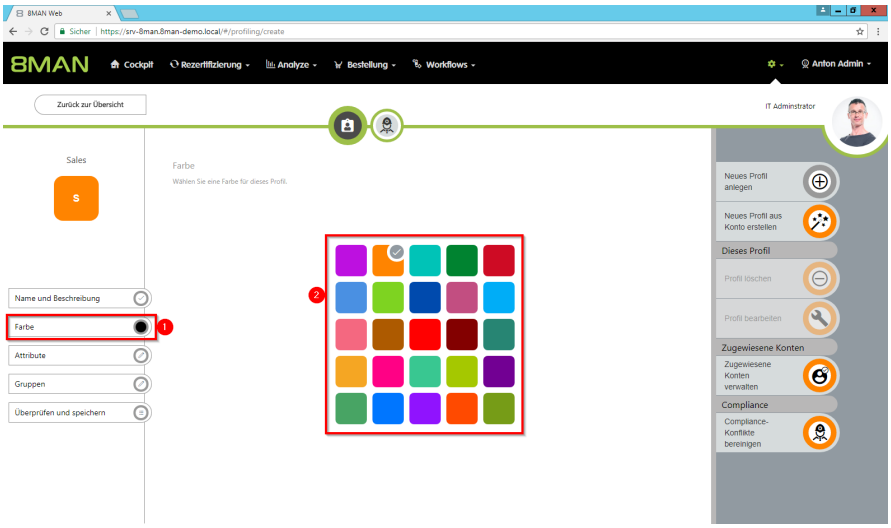
Sie müssen als 8MAN Administrator eingeloggt sein, um das Zahnradsymbol sehen zu können.



Klicken Sie auf "Neues Profil anlegen".

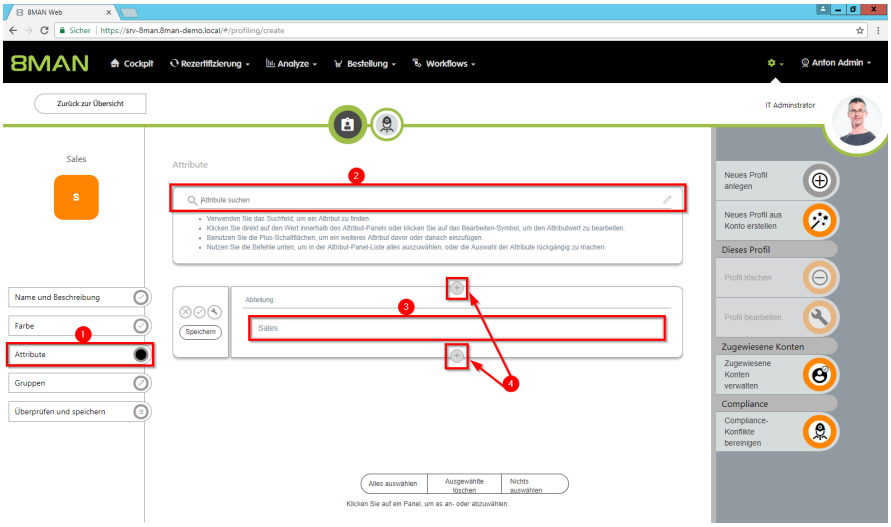


1. *Geben Sie dem Abteilungsprofil einen Namen, mindestens 3 Buchstaben.*
2. *Optional: Beschreiben Sie das Profil.*

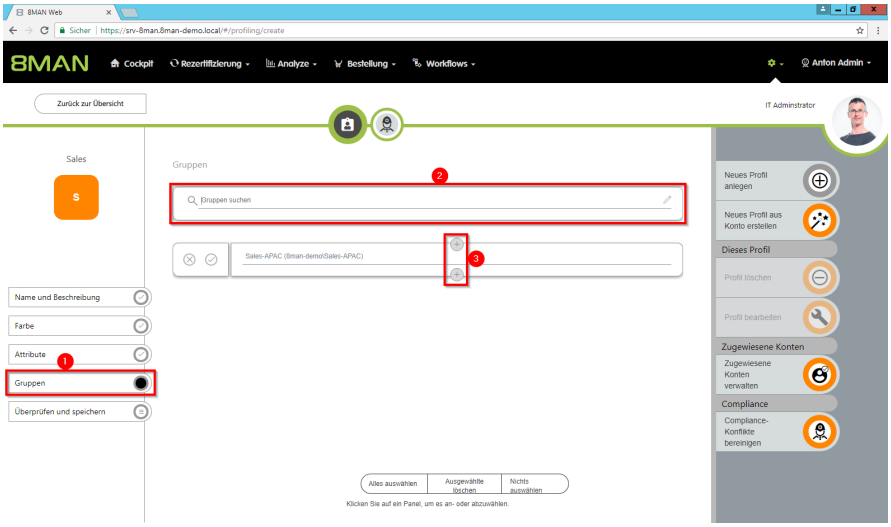


1. *Klicken Sie auf "Farbe".*
2. *Wählen Sie eine Farbe für das Abteilungsprofil.*

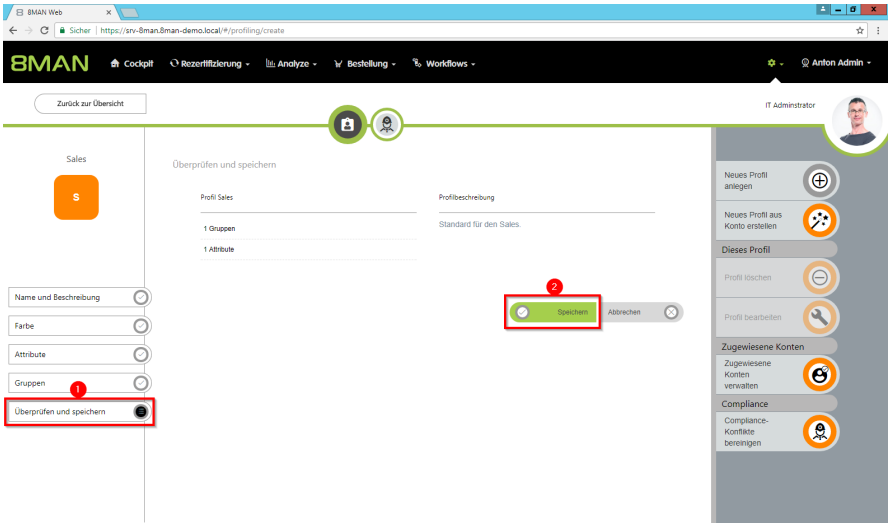
Die Farbe dient der Wiedererkennung.



1. *Klicken Sie auf "Attribute".*
2. *Nutzen Sie die Suche, um das gewünschte Attribut zu finden.*
3. *Tragen Sie den Wert des Attributes ein.*
4. *Nutzen Sie die Plus-Symbole, um weitere Attribute hinzuzufügen.*



1. *Kicken Sie auf "Gruppen".*
2. *Suchen Sie die gewünschte Gruppe.*
3. *Nutzen Sie die Plus-Symbole, um weitere Gruppen hinzuzufügen.*



1. *Klicken Sie auf "Überprüfen und speichern".*
2. *Klicken Sie auf "Speichern", um das Abteilungsprofil zu erstellen.*

8.1.1.17 Skripte für Verzeichnisse im Bulk ausführen

Hintergrund / Mehrwert

Verwenden Sie selbst erstellte Skripte auf Verzeichnisse. Damit eröffnet 8MAN Raum für sehr individuelle Anforderungen. Legen Sie ihre Skripte im folgenden Verzeichnis ab, um sie mit 8MAN zu verwenden:

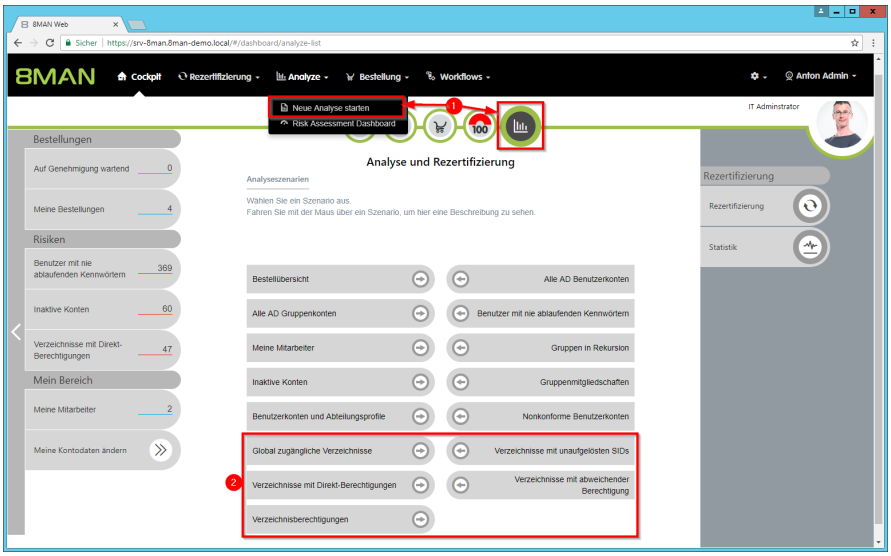
%ProgramData%\protected-networks.com\8MAN\scripts\analyze

Weitere notwendige Schritte und Details zur Konfiguration von Skripten finden Sie im Installations- und Konfigurationshandbuch.

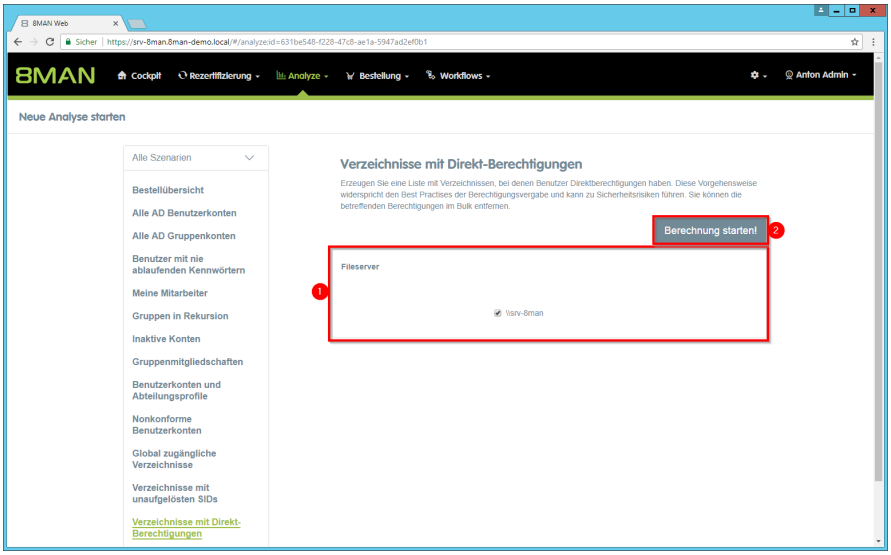
Weiterführende Services

Skripte für Nutzerkonten im Bulk ausführen (Webclient)

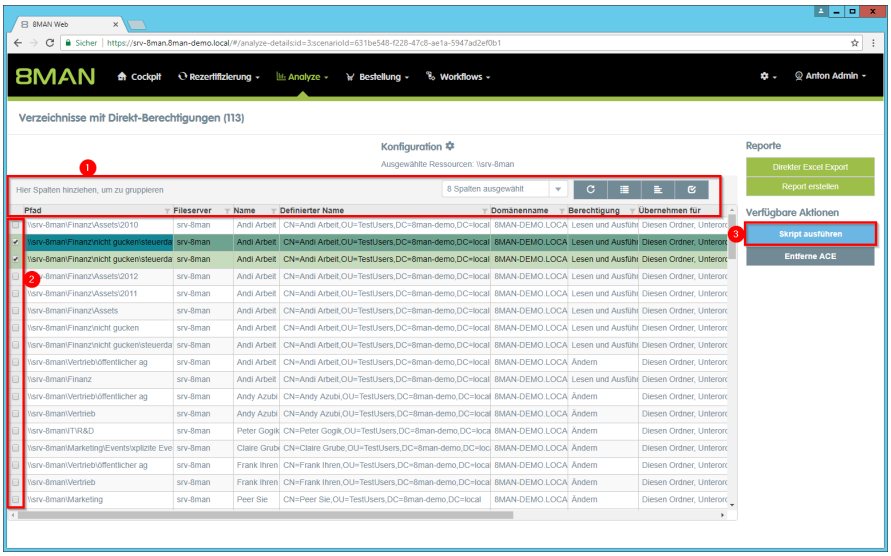
Der Prozess in einzelnen Schritten



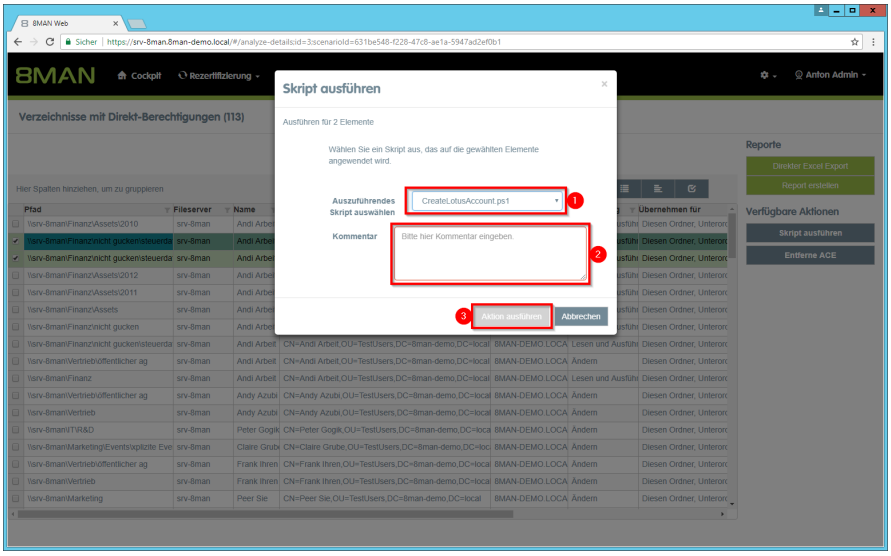
1. *Wählen Sie "Neue Analyse starten".*
2. *Wählen Sie ein Szenario mit Verzeichnissen im Fokus.*



1. *Legen Sie die Szenario-Optionen fest.*
2. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie die Gruppierungs-, Sortier- und Filterfunktion, um Ihr Ergebnis einzugrenzen.*
2. *Selektieren Sie die gewünschten Verzeichnisse.*
3. *Klicken Sie auf "Skript ausführen".*



1. *Wählen Sie ein Skript aus.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Klicken Sie auf "Aktion ausführen".*

8.1.1.18 Skripte für Nutzerkonten im Bulk ausführen

Hintergrund / Mehrwert

Verwenden Sie selbst erstellte Skripte auf Nutzerkonten oder Gruppen. Damit eröffnet 8MAN Raum für sehr individuelle Anforderungen. Legen Sie ihre Skripte im folgenden Verzeichnis ab, um sie mit 8MAN zu verwenden:

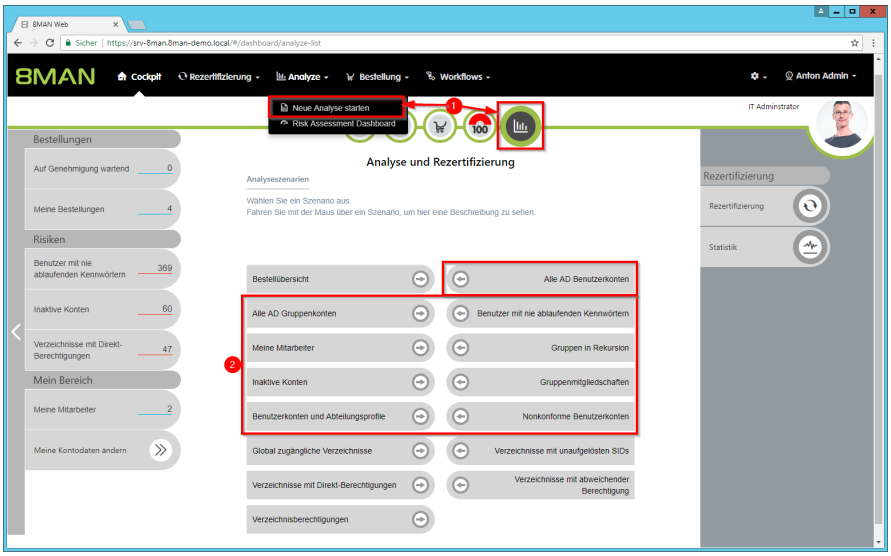
%ProgramData%\protected-networks.com\8MAN\scripts\analyze

Weitere notwendige Schritte und Details zur Konfiguration von Skripten finden Sie im Installations- und Konfigurationshandbuch.

Weiterführende Services

Scripte für Verzeichnisse im Bulk ausführen (Webclient)

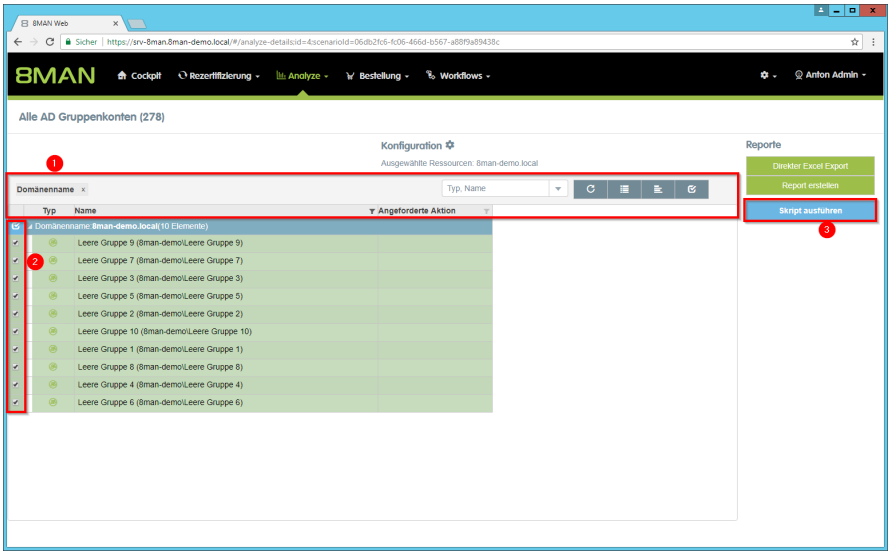
Der Prozess in einzelnen Schritten



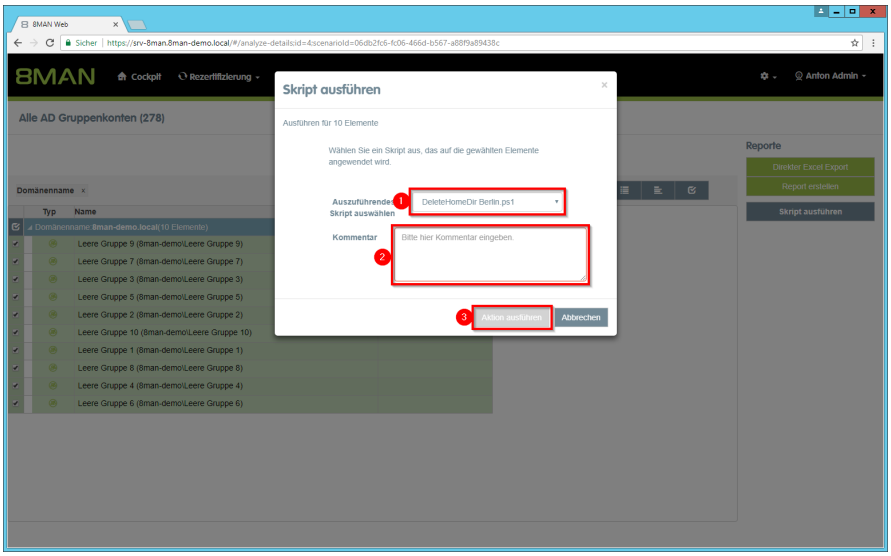
1. *Wählen Sie "Neue Analyse starten".*
2. *Wählen Sie ein Szenario mit Konten im Fokus.*

e

1. *Legen Sie die Szenario-Optionen fest.*
2. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie die Gruppierungs-, Sortier- und Filterfunktion, um Ihr Ergebnis einzugrenzen.*
2. *Selektieren Sie die gewünschten Verzeichnisse.*
3. *Klicken Sie auf "Skript ausführen".*



1. *Wählen Sie ein Skript aus.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Klicken Sie auf "Aktion ausführen".*

8.1.1.19 Temporäre Gruppenmitgliedschaften bearbeiten (Webclient)

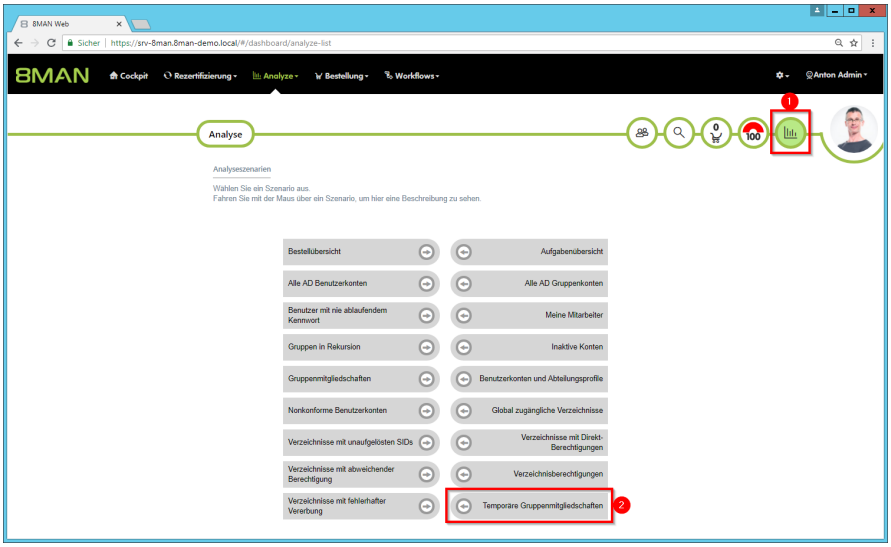
Hintergrund / Mehrwert

Ändern Sie einfach das Ablaufdatum von temporären Gruppenmitgliedschaften oder wandeln sie in eine dauerhafte Mitgliedschaft um. Sie können temporäre Mitgliedschaften auch einfach entfernen.

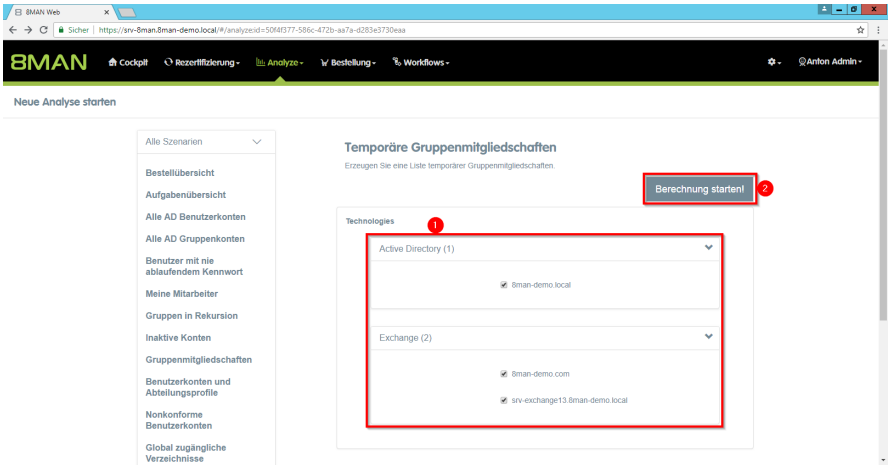
Ähnliche Services

Gruppenmitgliedschaften entfernen (Cockpit)
Gruppenmitgliedschaften hinzufügen (Cockpit)

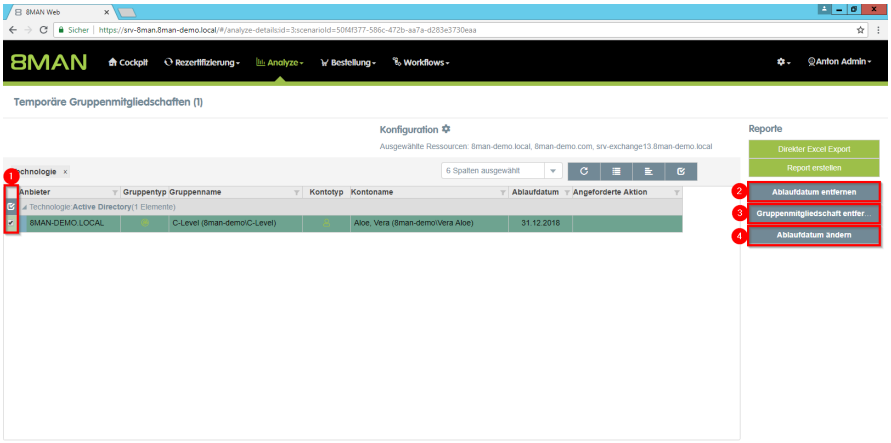
Der Prozess in einzelnen Schritten



1. *Wählen Sie im Cockpit "Analyse".*
2. *Klicken Sie auf "Temporäre Gruppenmitgliedschaften".*



1. *Wählen Sie die Ressourcen aus, die in Ihrer Analyse enthalten sein sollen.*
2. *Starten Sie das Szenario.*



1. *Selektieren Sie die gewünschten Gruppenmitgliedschaften.*
2. *Entfernen Sie das Ablaufdatum. So wandeln Sie die temporäre in eine dauerhafte Gruppenmitgliedschaft um.*
3. *Beenden Sie die Gruppenmitgliedschaft sofort (vor dem Ablaufdatum).*
4. *Ändern Sie das Ablaufdatum.*

8.1.1.20 Computerkonten editieren

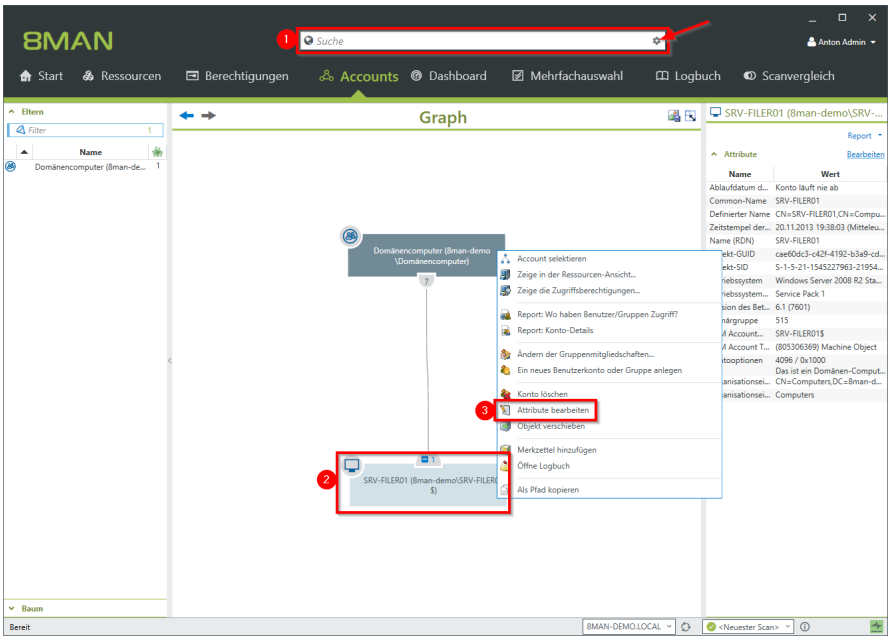
Hintergrund / Mehrwert

Pflegen Sie Computerkonten komfortabel und dokumentiert innerhalb 8MAN.

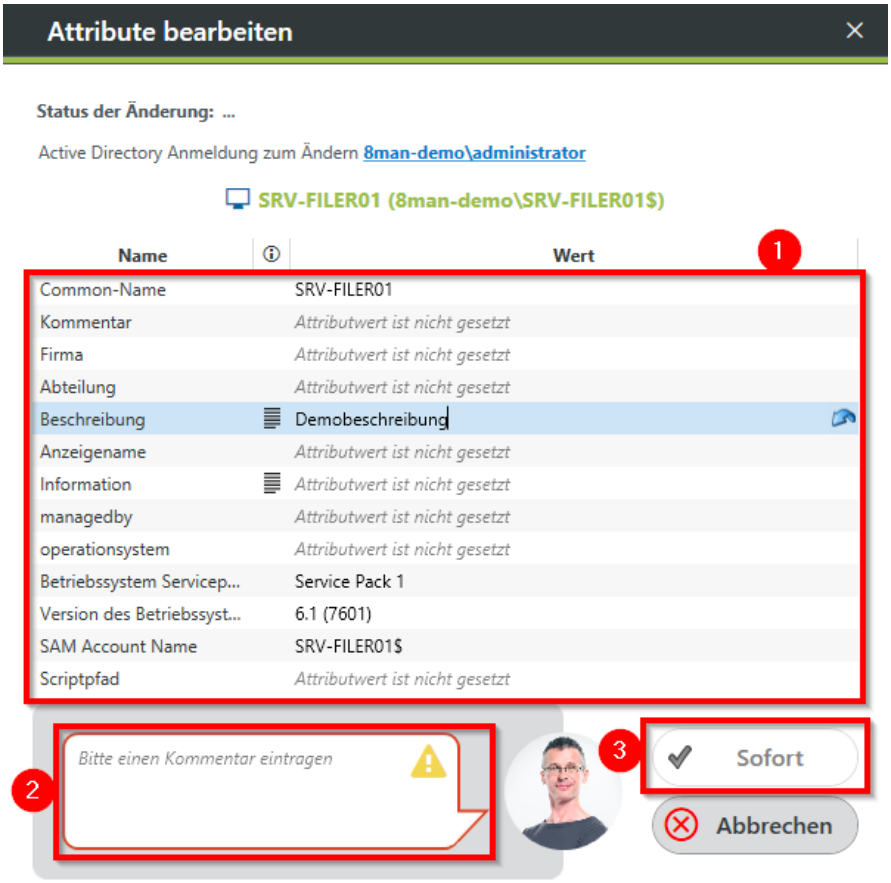
Weiterführende Services

Computerkonten löschen

Der Prozess in einzelnen Schritten



1. *Suchen Sie ein Computerkonto. In den Suchoptionen (Pfeil) müssen Computerkonten aktiviert sein.*
2. *Rechtsklicken Sie das gefundene Computerkonto.*
3. *Wählen Sie "Attribute bearbeiten".*



1. *Ändern Sie die Attribute. 8MAN lädt ein Standardset von Attributen. Sollen weitere Attribute von Computerkonten in 8MAN geladen werden, wenden Sie sich bitte an unseren Support.*
2. *Sie müssen einen Kommentar angeben.*
3. *Starten Sie die Ausführung.*

8.1.1.21 Computerkonten löschen

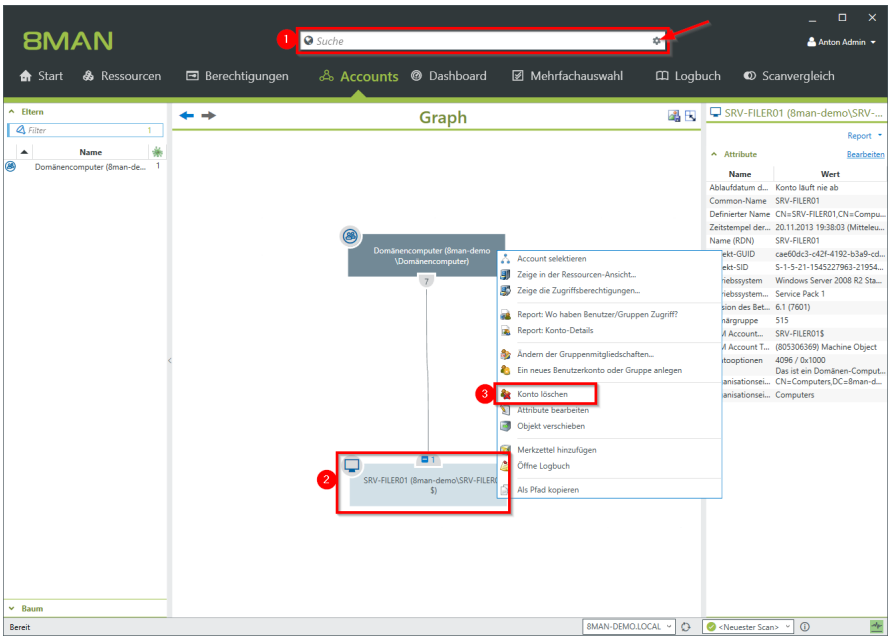
Hintergrund / Mehrwert

Löschen Sie Computerkonten komfortabel und dokumentiert innerhalb 8MAN.

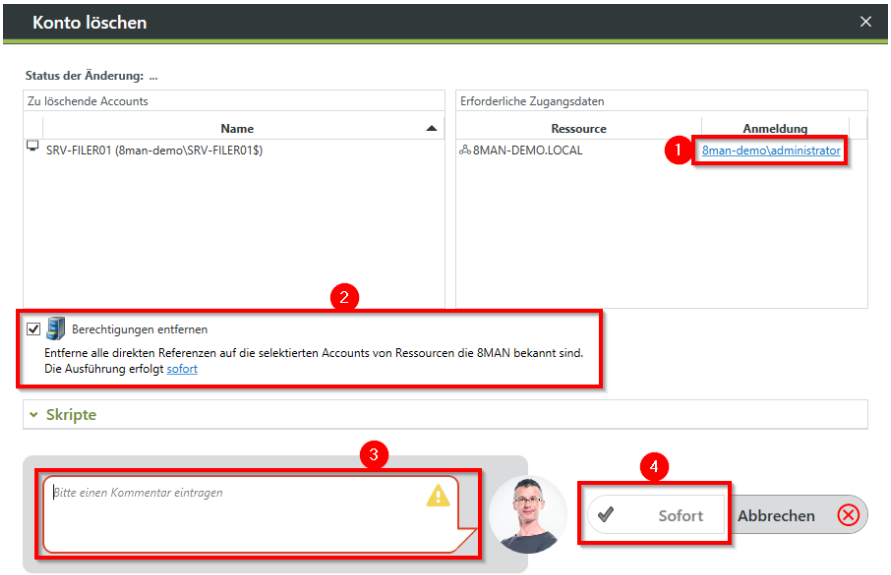
Weiterführende Services

Computerkonten editieren

Der Prozess in einzelnen Schritten



1. *Suchen Sie ein Computerkonto. In den Suchoptionen (Pfeil) müssen Computerkonten aktiviert sein.*
2. *Rechtsklicken Sie das gefundene Computerkonto.*
3. *Wählen Sie "Konto löschen".*



1. *Optional: Ändern Sie die Anmeldung, mit der das Konto gelöscht werden soll.*
2. *Empfohlen: Aktivieren Sie die Option, um ggf. vorhandene (direkte) Berechtigungseinträge zu entfernen.*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie die Ausführung.*

8.1.2 Helpdesk

8.1.2.1 Ein Kennwort zurücksetzen

Hintergrund / Mehrwert

Das Zurücksetzen von Passwörtern zählt zu den am häufigsten durchgeführten Operationen im Helpdesk. 8MAN ermöglicht revisionssicheres Kennwort zurücksetzen. Die sicherheitskritische Aktion wird im Logbuch erfasst. Sollte ein Mitarbeiter mit Bordmitteln ein Passwort zurücksetzen, um sich illegal mit dem Konto anzumelden, wird der Vorfall vom 8MATE AD Logga erfasst.

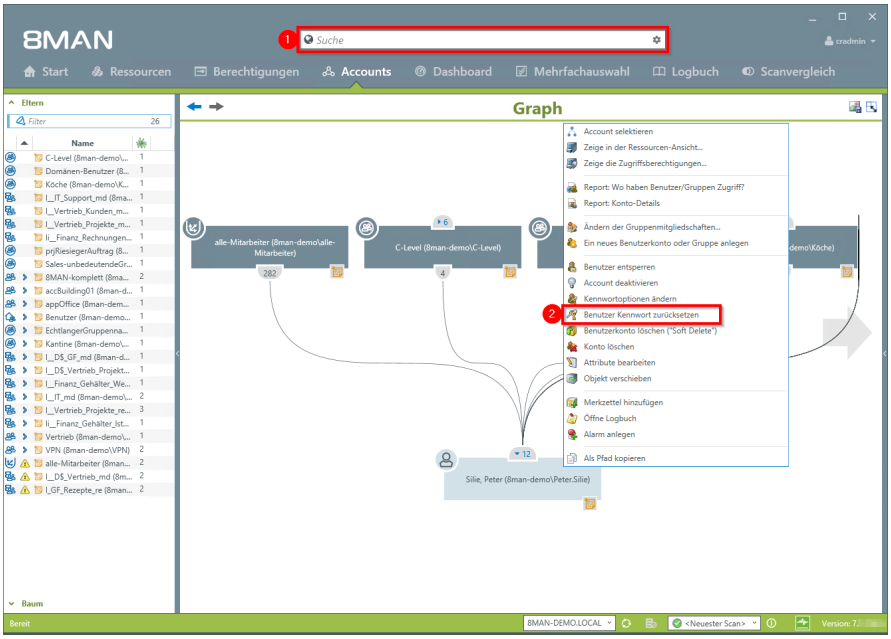
Besonders schützenswerte Nutzerkonten, können mit dem 8MATE AD Logga proaktiv überwacht werden.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.11 Regelung des Passwortgebrauchs sowie M 4.48 Passwortschutz unter Windows-Systemen.

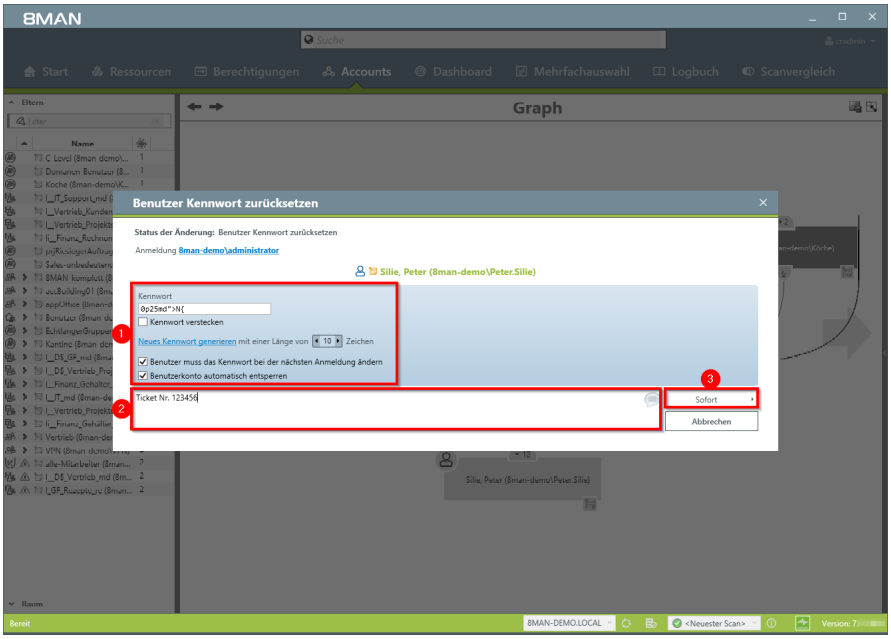
Weiterführende Services

8MATE AD Logga: Gesperrte Benutzerkonten identifizieren
8MATE AD Logga: Ein Nutzerkonto überwachen
Kennwörter im Bulk zurücksetzen (web client)

Der Prozess in einzelnen Schritten



1. *Finden Sie den gewünschten Benutzer mit der Suche.*
2. *Rechtsklicken Sie den Benutzer, z. B. in der Accounts-Ansicht und wählen "Benutzer Kennwort zurücksetzen" im Kontextmenü.*



1. *Legen Sie Kennwort-Optionen fest.*
2. *Sie müssen einen Kommentar eingeben, z. B. "Ticketnummer", "Beauftragt von" oder "Genehmigt von".*
3. *Starten Sie das Rücksetzen.*

8.1.2.2 Ein Konto entsperren (Webclient)

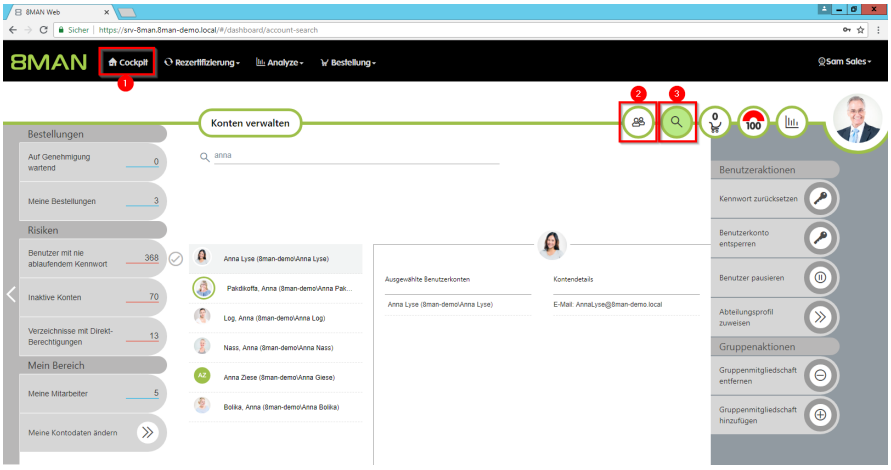
Hintergrund / Mehrwert

Die häufigste Tätigkeit des HelpDesks ist es, Konten zu entsperren. Typischerweise, weil das Kennwort zu oft falsch eingegeben wurde. Falls dem Nutzer das Kennwort wieder einfällt, kann das Konto entsperrt werden, ohne dass das Kennwort zurückgesetzt werden muss.

Ähnliche Services

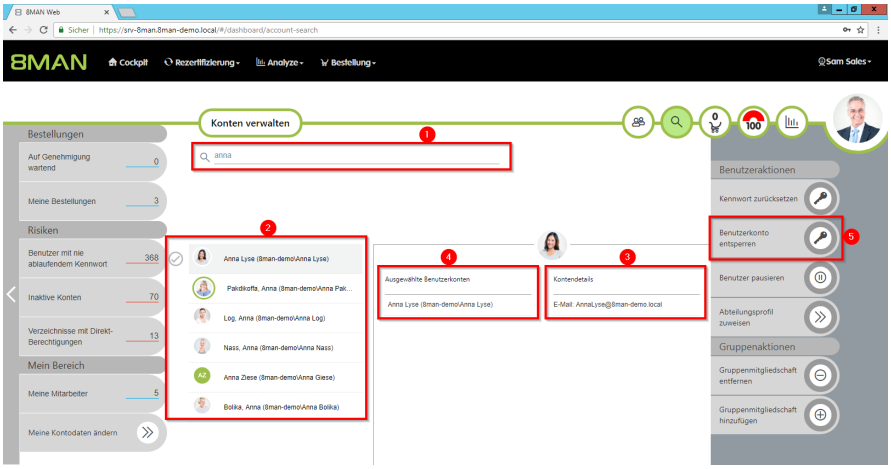
Kennwörter von Benutzern zurücksetzen (Cockpit)

Der Prozess in einzelnen Schritten

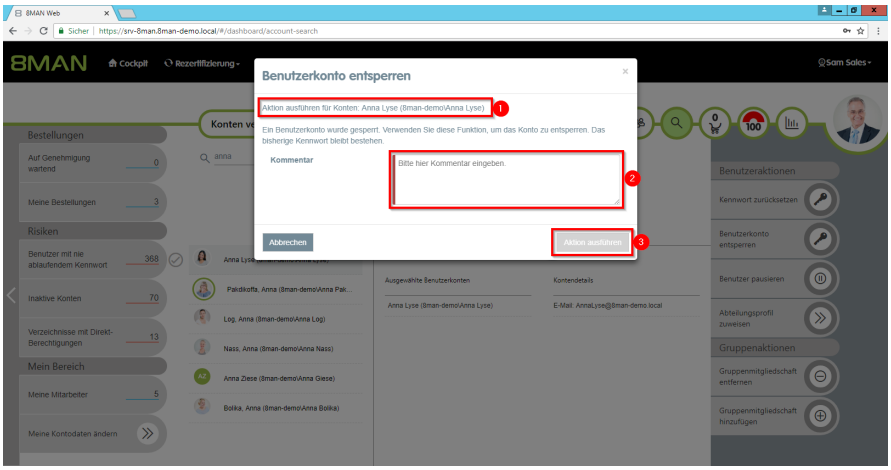


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter werden Ihnen von einem Administrator über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Benutzer verwalten. Benutzer werden Ihnen von einem Administrator über die Data-Owner-Konfiguration zugeordnet.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Benutzern zu suchen.*
2. *Wählen Sie einen oder mehrere Benutzer.*
3. *8MAN zeigt Ihnen die Informationen (Attribute) des ausgewählten Benutzers. Haben Sie mehrere Benutzer ausgewählt, werden Ihnen nur die gemeinsamen Attribute angezeigt.*
4. *In der Sammlung sehen Sie bereits ausgewählte Benutzer.*
5. *Klicken Sie auf "Benutzerkonto entsperren".*



1. *8MAN zeigt Ihnen, auf welche Konten die Aktion angewendet werden soll.*
2. *Sie müssen einen Kommentar angeben.*
3. *Klicken Sie auf "Aktion ausführen".*

8.1.2.3 Kennwörter im Bulk zurücksetzen (Webclient)

Hintergrund / Mehrwert

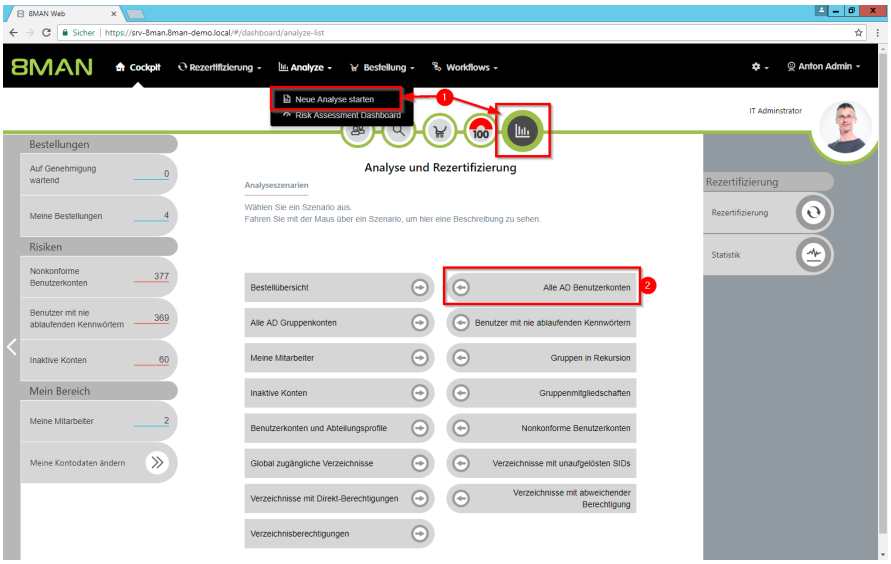
Ob eine neue Kennwort - Regulation oder ein Data Breach: Nicht selten müssen Passwörter von mehreren Usern gleichzeitig zurückgesetzt werden. Nutzen Sie dazu die Bulk Operation im neuen Webclient.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.11 Regelung des Passwortgebrauchs sowie M 4.48 Passwortschutz unter Windows-Systemen.

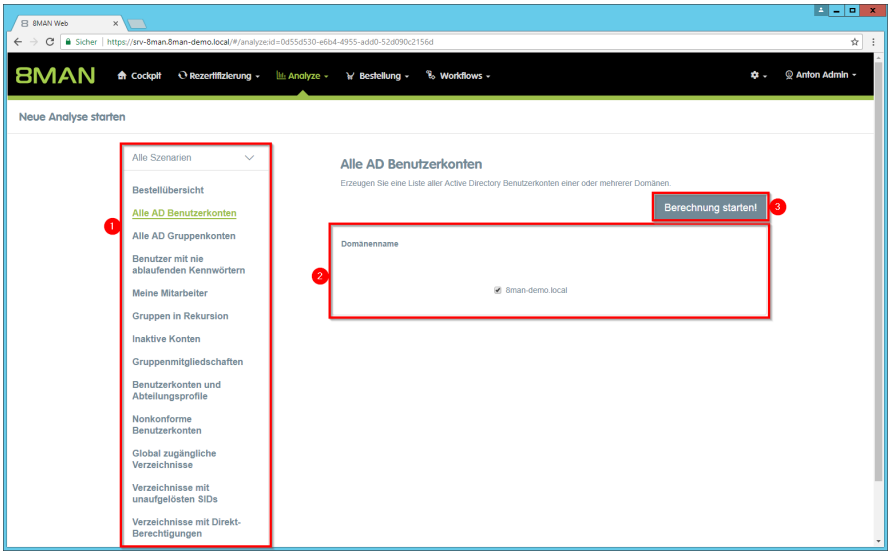
Weiterführende Services

Konten im Bulk deaktivieren (Webclient)
Kennwortoptionen im Bulk ändern (Webclient)

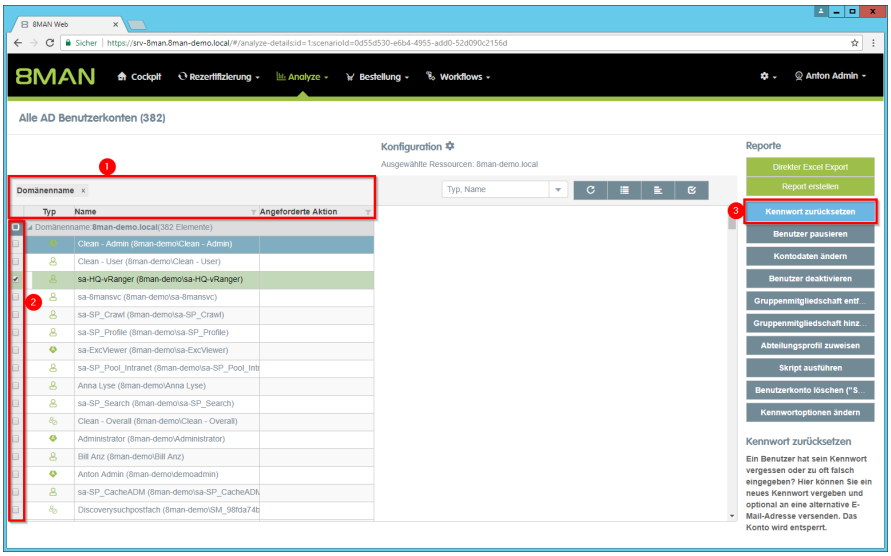
Der Prozess in einzelnen Schritten



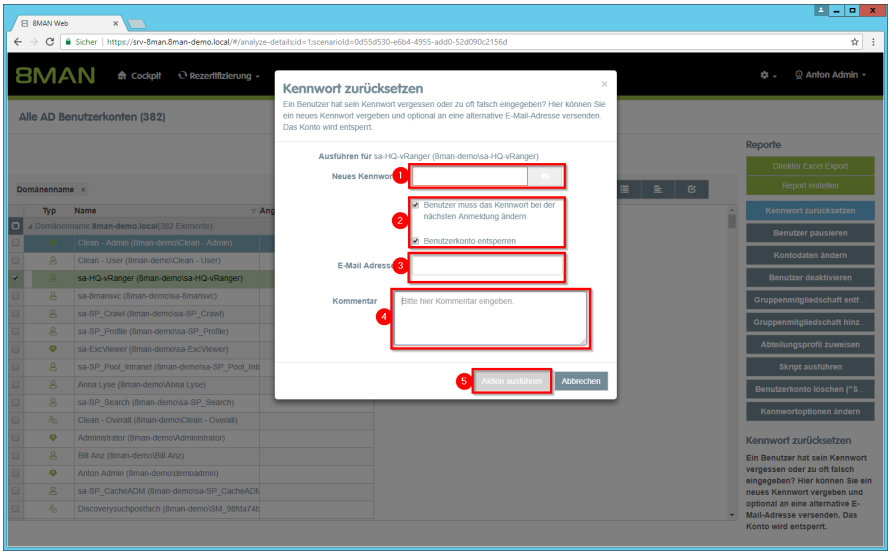
1. *Wählen Sie "Neue Analyse starten".*
2. *Klicken Sie auf "Alle AD Benutzerkonten".*



1. *Optional: Wechseln Sie das Szenario.*
2. *Legen Sie Optionen für das Szenario fest.*
3. *Klicken Sie auf "Berechnung starten".*



1. *Nutzen Sie Sortier-, Filter- und Gruppierungsfunktionen, um Ihre Auswahl einzugrenzen.*
2. *Selektieren Sie die gewünschten Einträge.*
3. *Klicken Sie auf "Kennwort zurücksetzen".*



1. *Vergeben Sie ein neues Kennwort.*
2. *Aktivieren Sie die gewünschten Optionen. Diese Optionen sind nur für 8MAN-Administratoren verfügbar. Für alle anderen 8MAN-Rollen sind diese Optionen nicht sichtbar und immer aktiviert.*
3. *Optional: Geben Sie ein E-Mail-Konto an, auf das die Benutzer zugreifen können.*
4. *Sie müssen einen Kommentar eingeben.*

5. *Klicken Sie auf "Aktion ausführen".*

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.

8.1.2.4 Einen Benutzer entsperren

Hintergrund / Mehrwert

Die Entsperrung von Nutzerkonten zählt zu den am häufigsten durchgeführten Operationen im Helpdesk. Die sicherheitskritische Aktion wird im Logbuch erfasst.

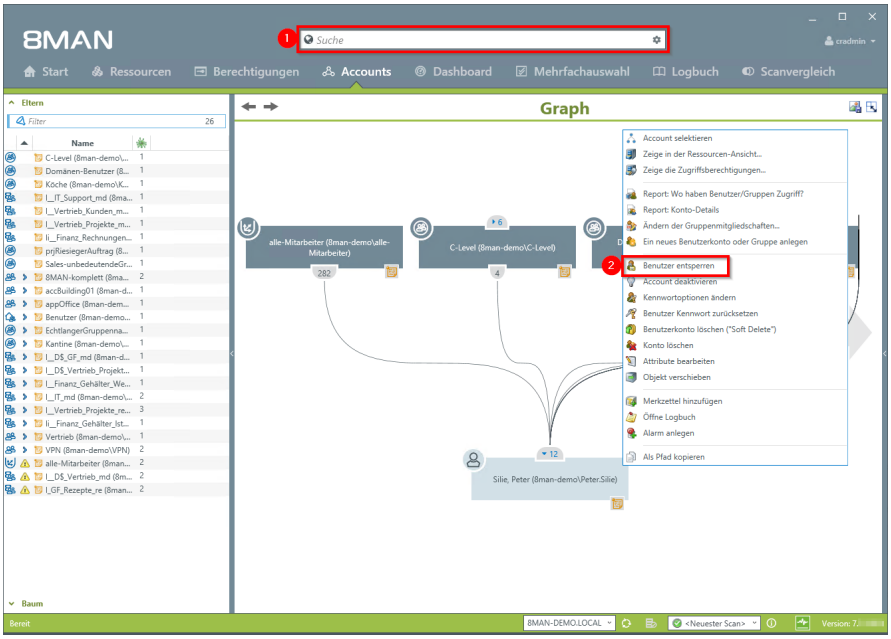
Weiterführende Services

Sollte ein Mitarbeiter mit Bordmitteln ein sicherheitskritisches Nutzerkonto entsperren, wird der Vorfall vom 8MATE AD Logga erfasst. Besonders schützenswerte Nutzerkonten überwachen Sie proaktiv mit den im AD Logga enthaltenen Alarmen.

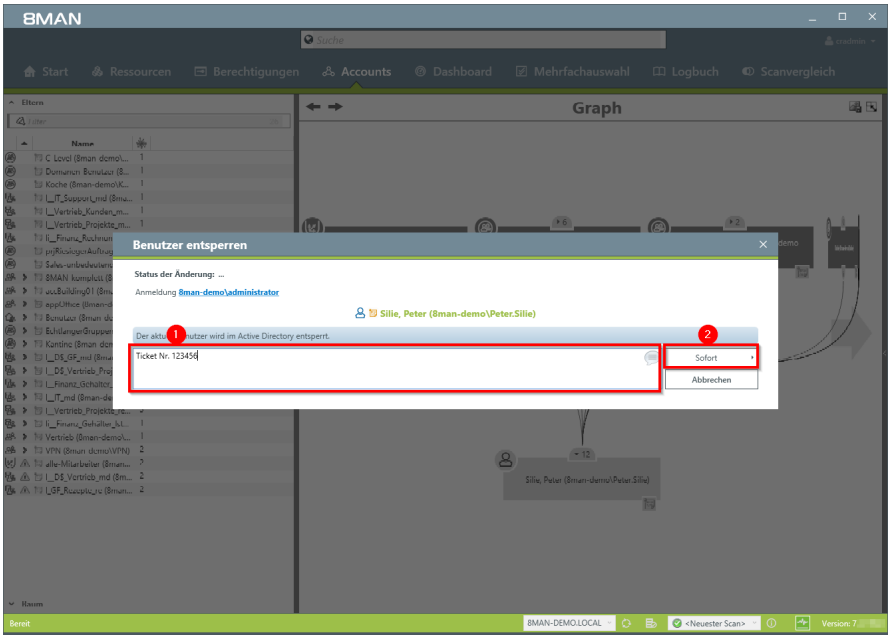
8MATE AD Logga: Gesperrte Benutzerkonten identifizieren.

8MATE AD Logga: Ein Nutzerkonto überwachen.

Der Prozess in einzelnen Schritten



1. *Finden Sie den gewünschten Benutzer oder die Gruppe mit der Suche.*
2. *Rechtsklicken Sie den Benutzer oder die Gruppe, z. B. in der Accounts-Ansicht und wählen "Benutzer entsperren" im Kontextmenü.*



1. *Sie müssen einen Kommentar eingeben, z. B. "Ticketnummer", "Beauftragt von" oder "Genehmigt von"*
2. *Starten Sie das Entsperren.*

8.1.2.5 Einen Benutzer deaktivieren

Hintergrund / Mehrwert

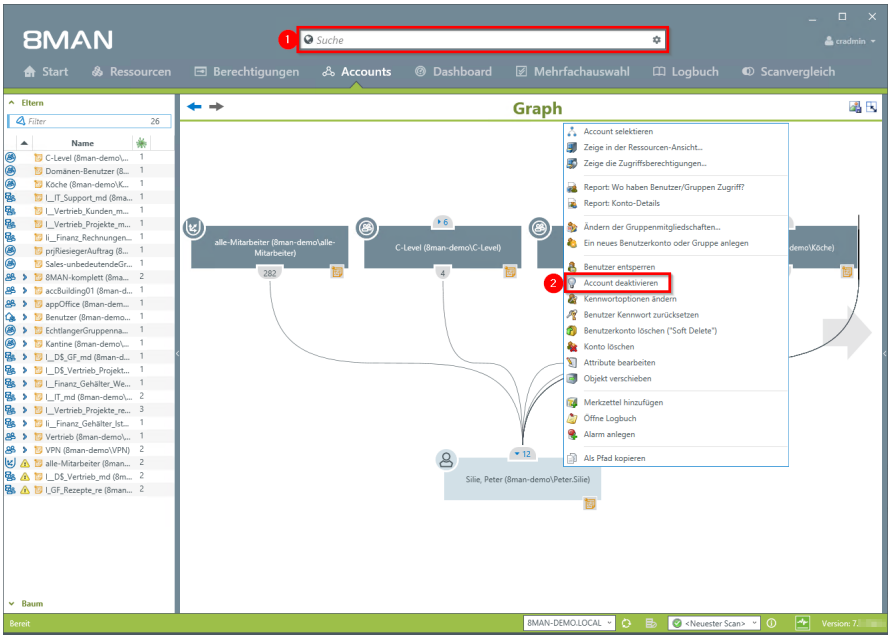
Deaktivieren Sie ein Konto in 8MAN, kommt es der normalen Deaktivierung im Active Directory gleich. Das Nutzerkonto bleibt in der OU.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.

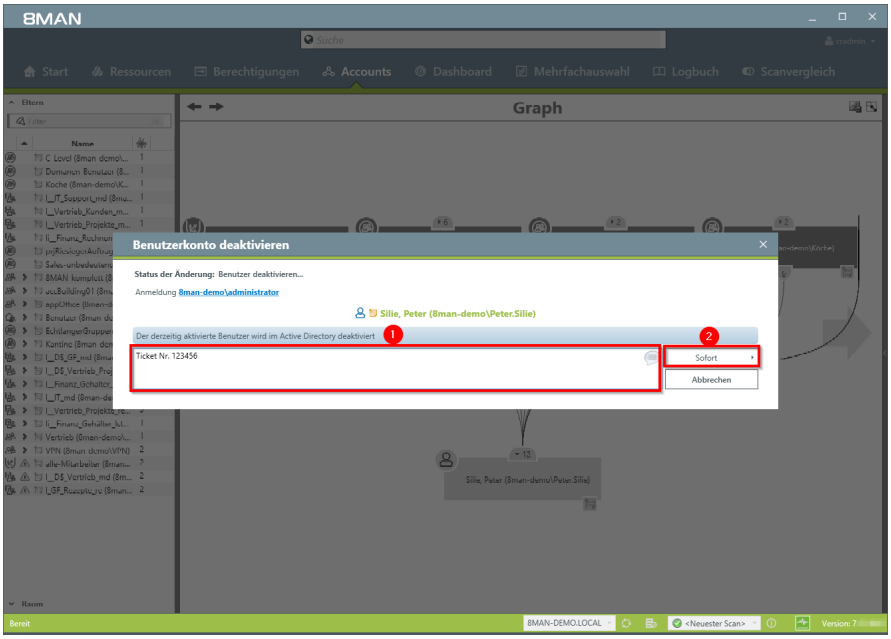
Weiterführende Services

Einen Nutzer mit Soft Delete löschen
Konten im Bulk deaktivieren (Webclient)

Der Prozess in einzelnen Schritten



1. *Finden Sie den gewünschten Benutzer mit der Suche.*
2. *Rechtsklicken Sie den Benutzer, z. B. in der Accounts-Ansicht und wählen "Account deaktivieren" im Kontextmenü.*



1. *Sie müssen einen Kommentar eingeben, z. B. "Ticketnummer", "Beauftragt von" oder "Genehmigt von"*
2. *Starten Sie die Ausführung.*

8.1.2.6 Attribute von Gruppen und Benutzerkonten bearbeiten

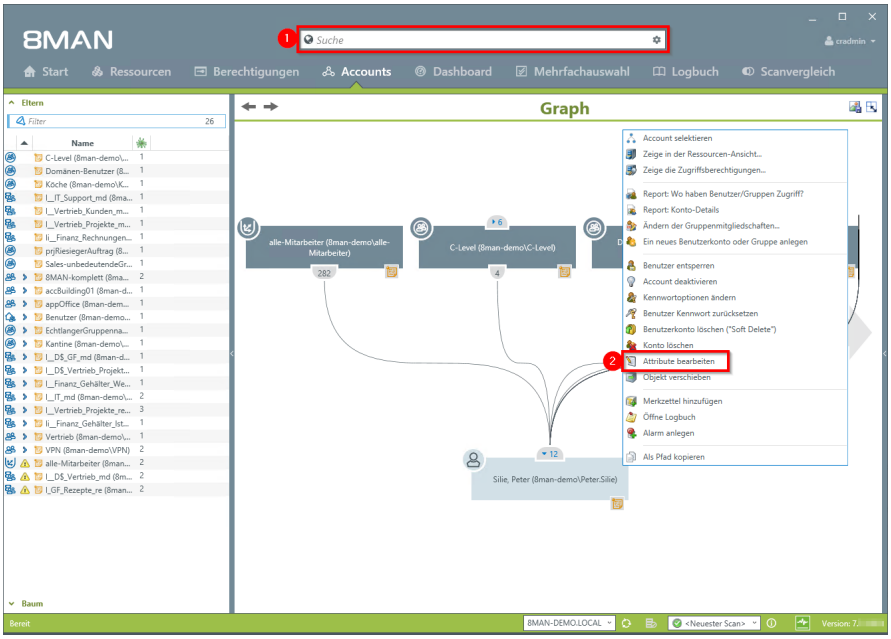
Hintergrund / Mehrwert

Mit 8MAN können Sie in einer flachen Liste schnell und komfortabel Attribute von Nutzerkonten ändern. Die Aktionen werden revisionssicher dokumentiert.

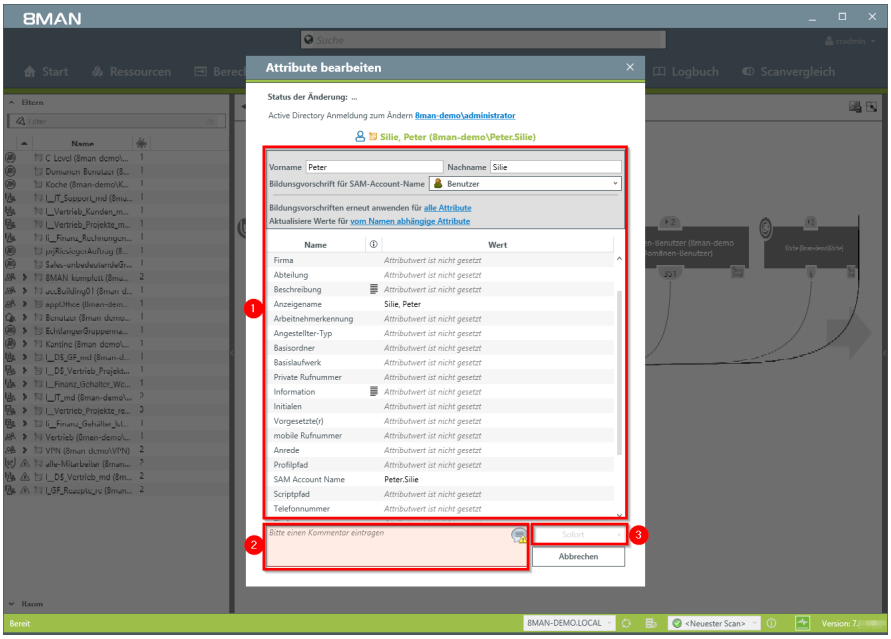
Weiterführende Services

Attribute im Bulk ändern (Webclient)

Der Prozess in einzelnen Schritten



1. *Finden Sie den gewünschten Benutzer oder die Gruppe mit der Suche.*
2. *Rechtsklicken Sie den Benutzer oder die Gruppe, z. B. in der Accounts-Ansicht.*



1. *Ändern Sie die Attribute.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie die Ausführung.*

8.1.2.7 Einen Benutzer mittels "Soft Delete" löschen

Hintergrund / Mehrwert

Löschen Sie einen Benutzer mit "Soft Delete", bleiben alle seine Berechtigungen erhalten. Das Konto wird in die Papierkorb-OU verschoben und deaktiviert.

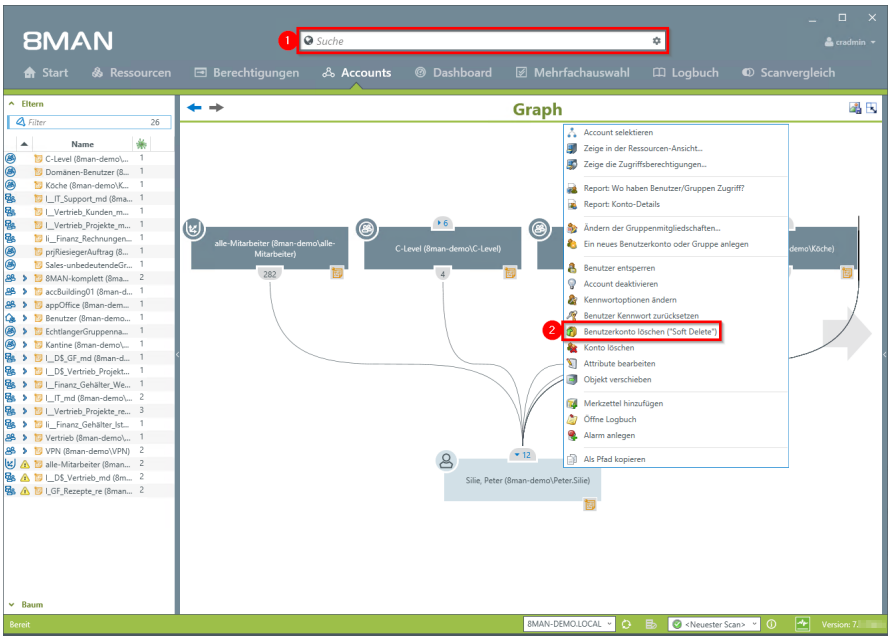
Damit kann das Konto nicht mehr missbraucht werden, da die Papierkorb-OU einer streng limitierten Group Policy unterliegt.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.

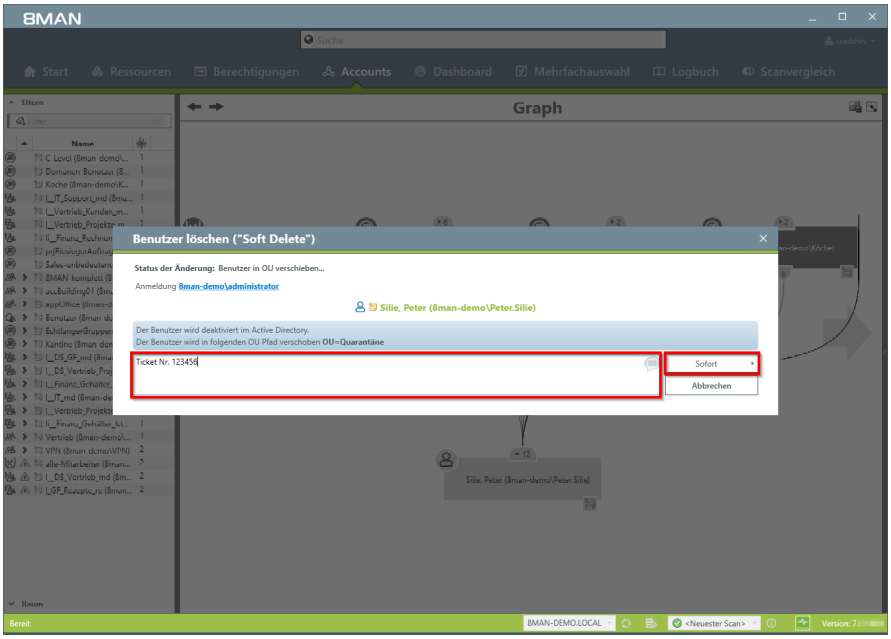
Weiterführende Services

Die Papierkorb-OU festlegen

Der Prozess in einzelnen Schritten



1. *Finden Sie den gewünschten Benutzer mit der Suche.*
2. *Rechtsklicken Sie den Benutzer, z. B. in der Accounts-Ansicht und wählen "Benutzerkonto löschen ("Soft Delete")" im Kontextmenü.*



1. *Sie müssen einen Kommentar eingeben, z. B. "Ticketnummer", "Beauftragt von" oder "Genehmigt von"*
2. *Starten Sie die Ausführung.*

8.1.2.8 Einen Nutzer und seine Berechtigungen löschen

Hintergrund / Mehrwert

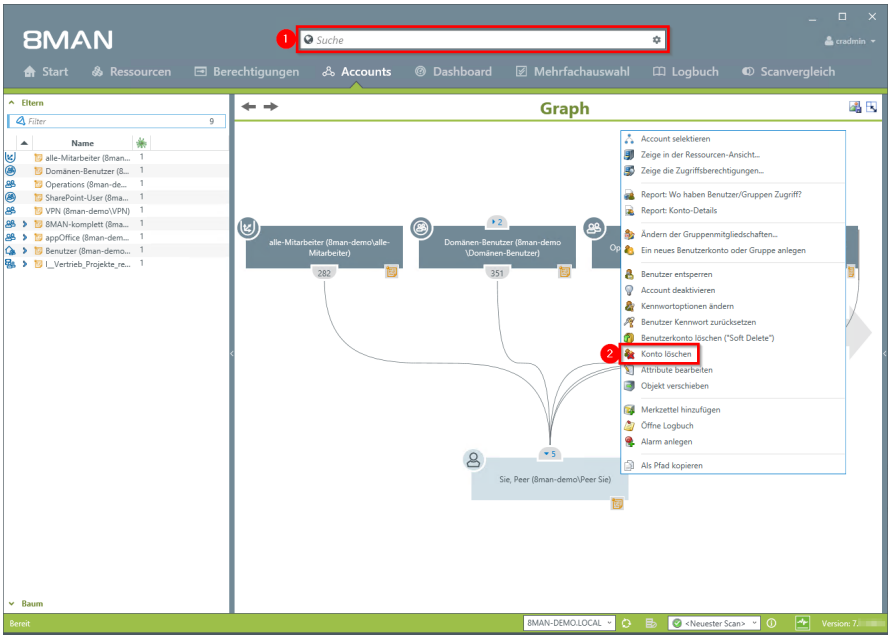
Mit 8MAN löschen Sie einen Nutzer aus dem AD und entfernen seine Direktberechtigungen auf dem Fileserver in einem Arbeitsgang.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.

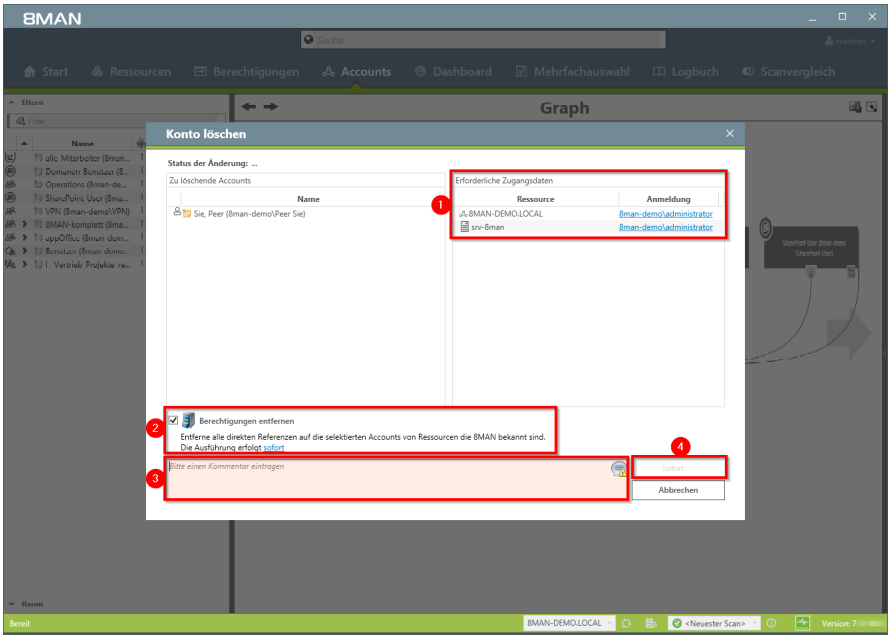
Weiterführende Services

Direktberechtigungen im Bulk entfernen (Webclient)

Der Prozess in einzelnen Schritten



1. *Finden Sie den gewünschten Benutzer mit der Suche.*
2. *Rechtsklicken Sie den Benutzer, z. B. in der Accounts-Ansicht und wählen "Konto löschen" im Kontextmenü.*



1. *Ändern Sie ggf. die Anmeldeinformationen zum Löschen bzw. Entfernen der Berechtigungen.*
2. *Aktivieren Sie die Option "Berechtigungen entfernen", um verwaiste SIDs auf Fileservern zu vermeiden.*
3. *Sie müssen einen Kommentar eingeben, z. B. "Ticketnummer", "Beauftragt von" oder "Genehmigt von".*
4. *Starten Sie das Löschen.*

8.1.3 Data Owner/Manager

8.1.3.1 Kennwörter von Benutzern zurücksetzen (Cockpit)

Hintergrund / Mehrwert

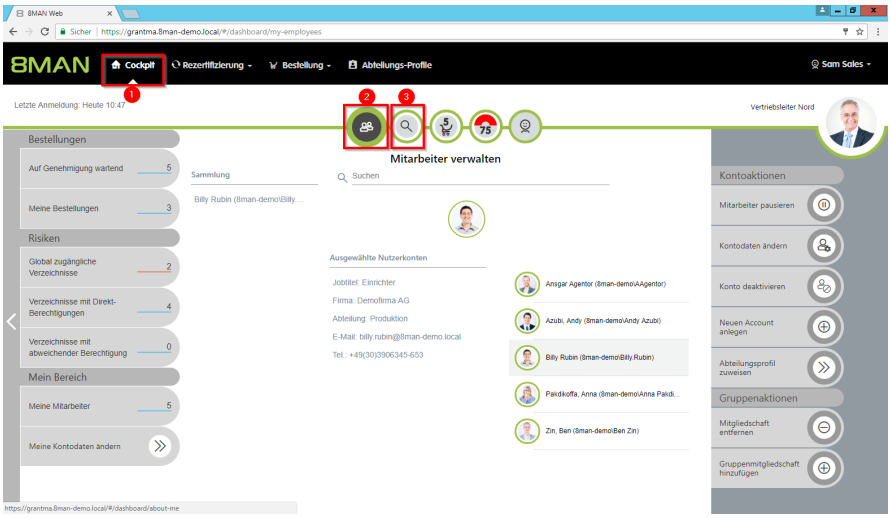
Das Zurücksetzen von Passwörtern zählt zu den am häufigsten durchgeführten Operationen im Helpdesk. 8MAN ermöglicht revisionssicheres Kennwort zurücksetzen. Die sicherheitskritische Aktion wird im Logbuch erfasst.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.11 Regelung des Passwortgebrauchs sowie M 4.48 Passwortschutz unter Windows-Systemen.

Weiterführende Services

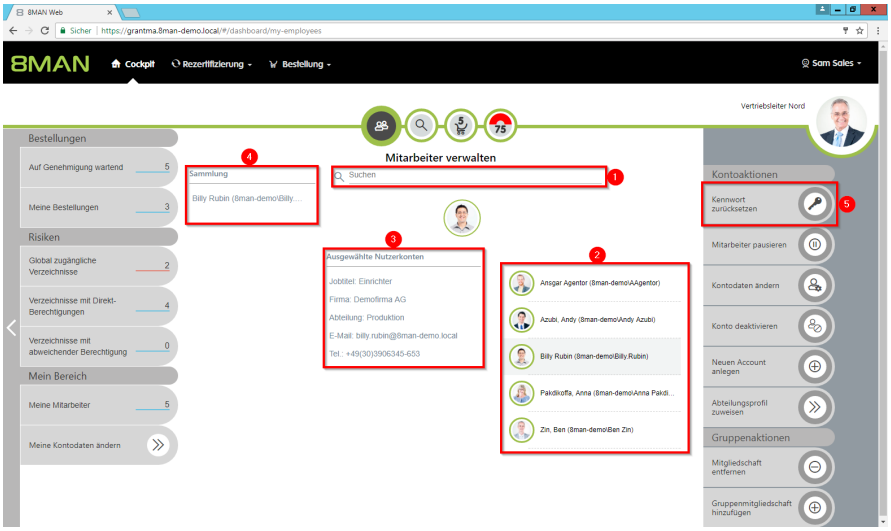
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

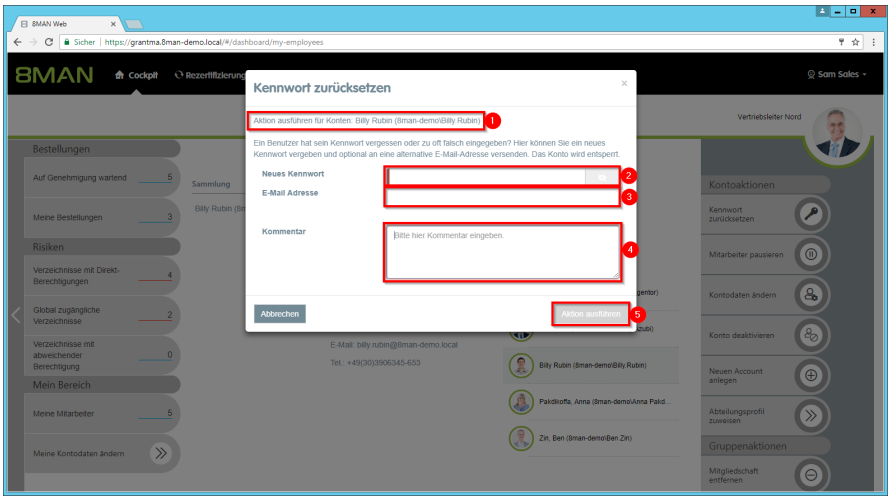


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter werden Ihnen von einem Administrator über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Benutzer verwalten. Benutzer werden Ihnen von einem Administrator über die Data-Owner-Konfiguration zugeordnet.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Benutzern zu suchen.*
2. *Wählen Sie einen oder mehrere Benutzer.*
3. *8MAN zeigt Ihnen die Informationen (Attribute) des ausgewählten Benutzers. Haben Sie mehrere Benutzer ausgewählt, werden Ihnen nur die gemeinsamen Attribute angezeigt.*
4. *In der Sammlung sehen Sie bereits ausgewählte Benutzer.*
5. *Klicken Sie auf "Kennwort zurücksetzen".*



1. *8MAN zeigt Ihnen, welche Benutzer Sie ausgewählt haben und deren Kennwörter Sie zurücksetzen.*
2. *Vergeben Sie ein Kennwort. Dieses Kennwort muss der Benutzer bei der ersten Anmeldung ändern.*
3. *Optional: Geben Sie eine E-Mail-Adresse an, an die das Kennwort versendet wird.* **Wählen Sie eine E-Mail-Adresse, die der Benutzer noch empfangen kann**.
4. *Sie müssen einen Grund für die Kennwortrücksetzung angeben.*
5. *Klicken Sie auf "Aktion ausführen".*

8.1.3.2 Kontodaten von Benutzern ändern (Cockpit)

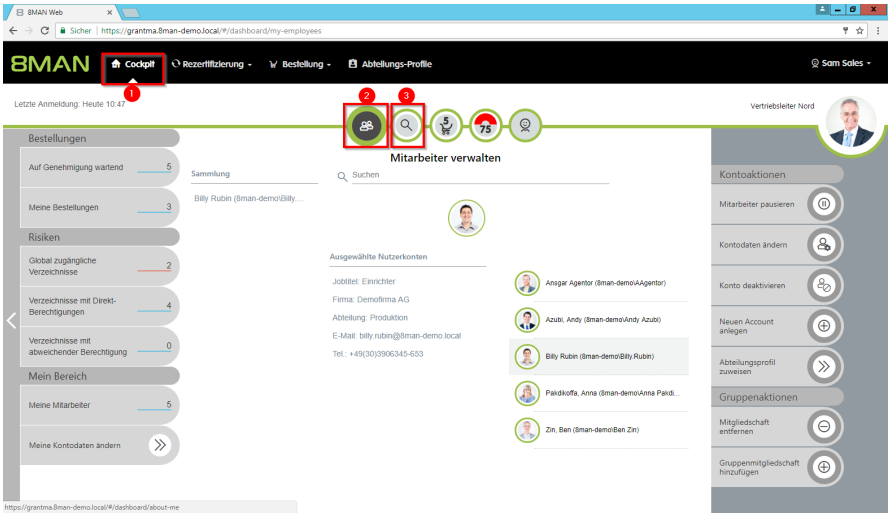
Hintergrund / Mehrwert

Mit 8MAN können Sie schnell und komfortabel Kontoinformationen von Benutzern ändern, auch von mehreren in einem Arbeitsgang. Die Aktionen werden revisionssicher dokumentiert.

Weiterführende Services

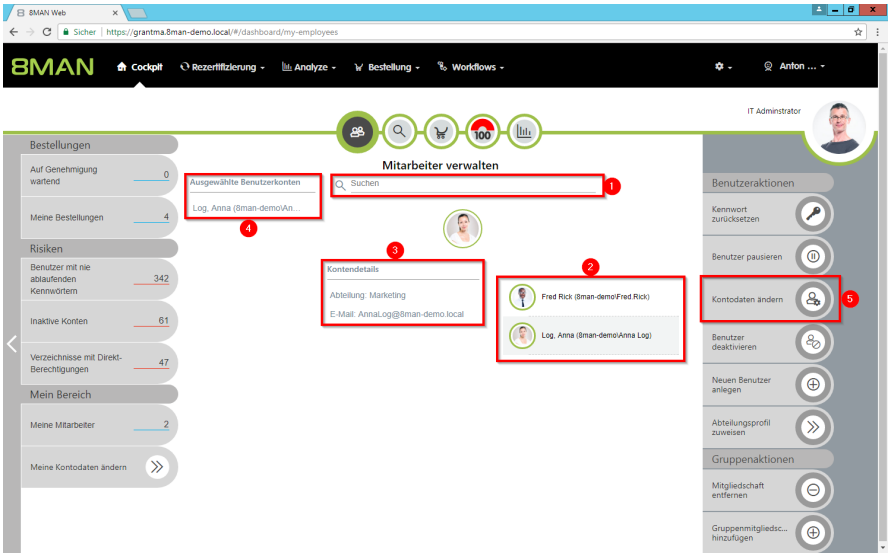
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten



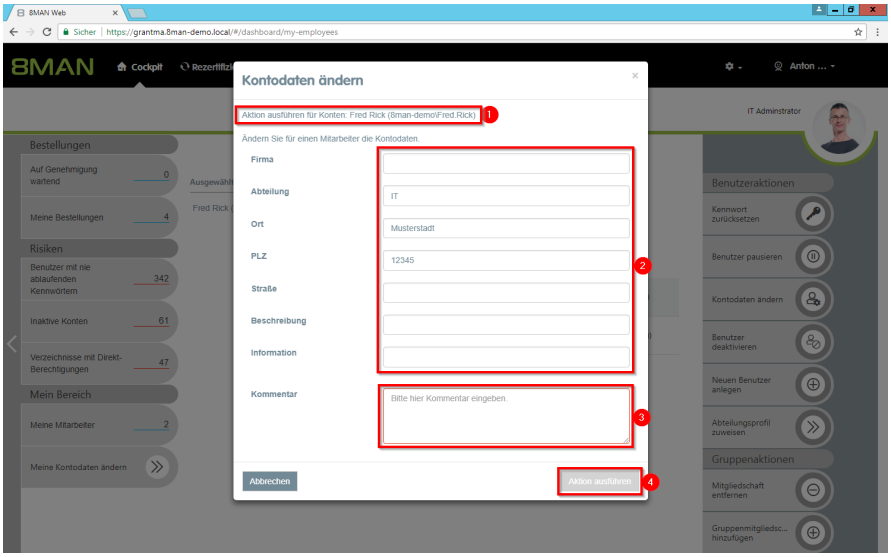
1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Konten zu suchen.*
2. *Wählen Sie einen oder mehrere Mitarbeiter/Konten.*
3. *8MAN zeigt Ihnen die Informationen (Attribute) des ausgewählten Kontos. Haben Sie mehrere Konten ausgewählt, werden Ihnen nur die gemeinsamen Attribute angezeigt.*

4. *In der Sammlung sehen Sie bereits ausgewählte Konten.*
5. *Klicken Sie auf "Kontodaten ändern".*



1. *8MAN zeigt Ihnen, welche Konten Sie ausgewählt haben.*
2. *Geben Sie die gewünschten Änderungen ein.*
3. *Sie müssen einen Kommentar angeben.*
4. *Klicken Sie auf "Aktion ausführen".*

Die in dem Dialog angezeigten Attribute können pro Rolle von einem Administrator angepasst werden. Dazu muss eine Anpassung der Konfigurationsdatei vorgenommen werden. Eine Anleitung finden Sie in unserer Knowledgebase (Login erforderlich).

8.1.3.3 Benutzer deaktivieren (Cockpit)

Hintergrund / Mehrwert

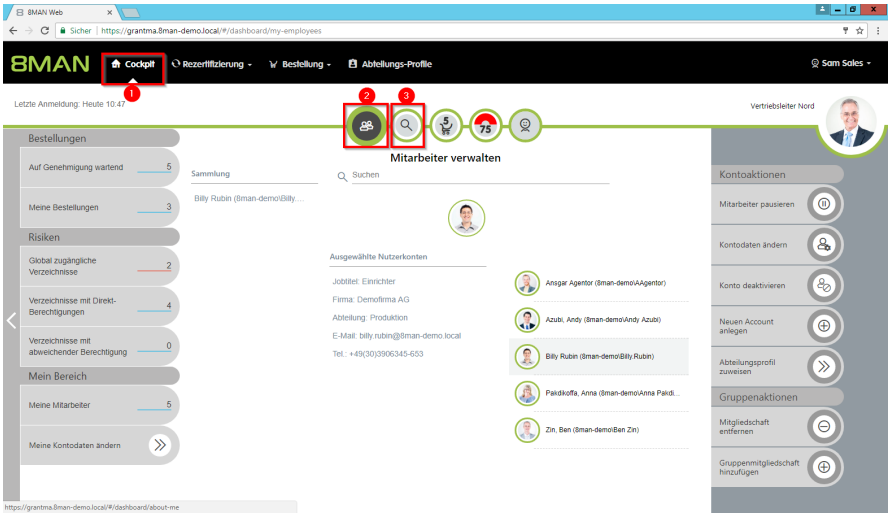
Deaktivieren Sie mit 8MAN einen Benutzer in wenigen Schritten. Deaktivieren Sie bei einer Entlassung frühzeitig ein Nutzerkonto.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.

Weiterführende Services

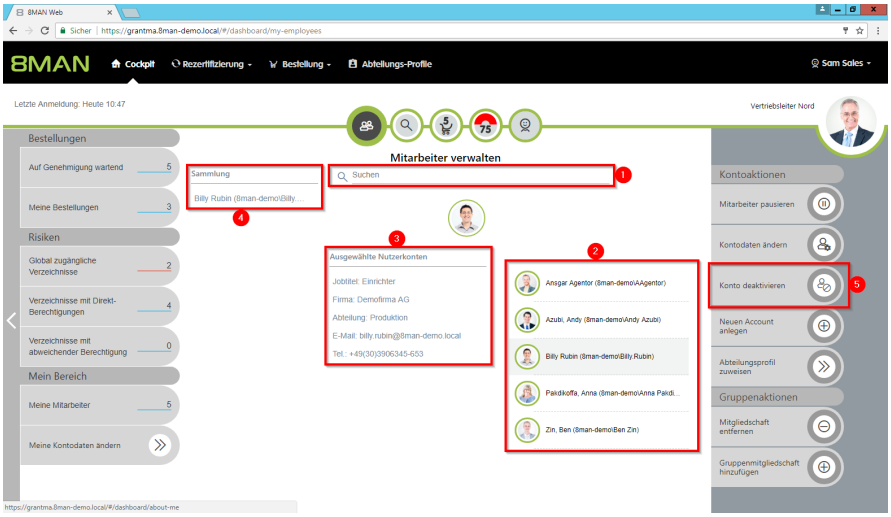
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

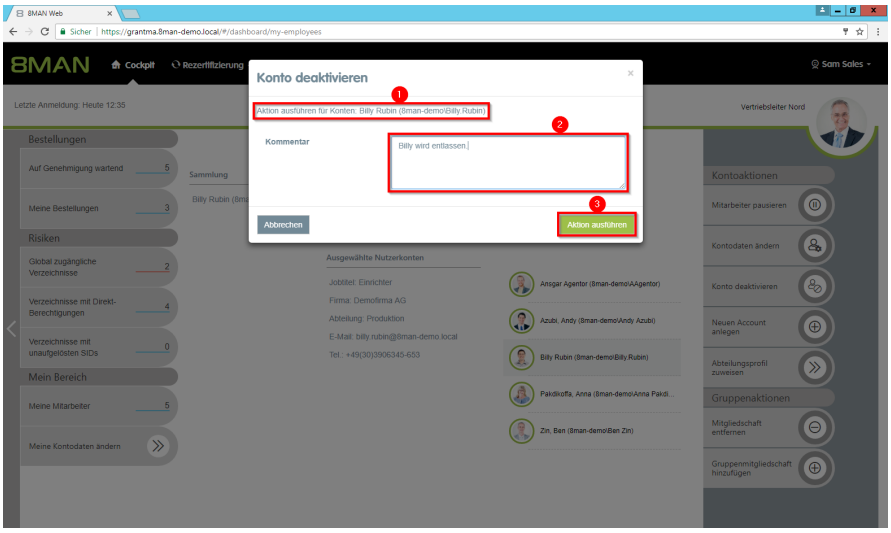


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Konten zu suchen.*
2. *Wählen Sie einen oder mehrere Mitarbeiter/Konten.*
3. *8MAN zeigt Ihnen die Informationen (Attribute) des ausgewählten Kontos. Haben Sie mehrere Konten ausgewählt, werden Ihnen nur die gemeinsamen Attribute angezeigt.*
4. *In der Sammlung sehen Sie bereits ausgewählte Konten.*
5. *Klicken Sie auf "Konto deaktivieren".*



1. *8MAN zeigt Ihnen, welche Konten Sie ausgewählt haben und deaktivieren wollen.*
2. *Sie müssen einen Kommentar angeben.*
3. *Klicken Sie auf "Aktion ausführen".*

8.1.3.4 Benutzer pausieren (Cockpit)

Hintergrund / Mehrwert

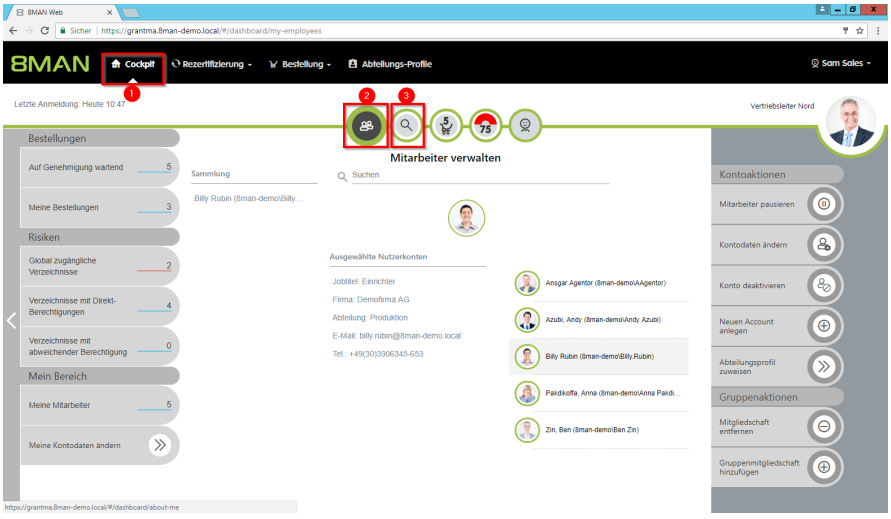
Pausieren Sie einen Mitarbeiter in wenigen einfachen und schnellen Schritten, z. B. bei Elternzeit.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen sowie M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern.

Weiterführende Services

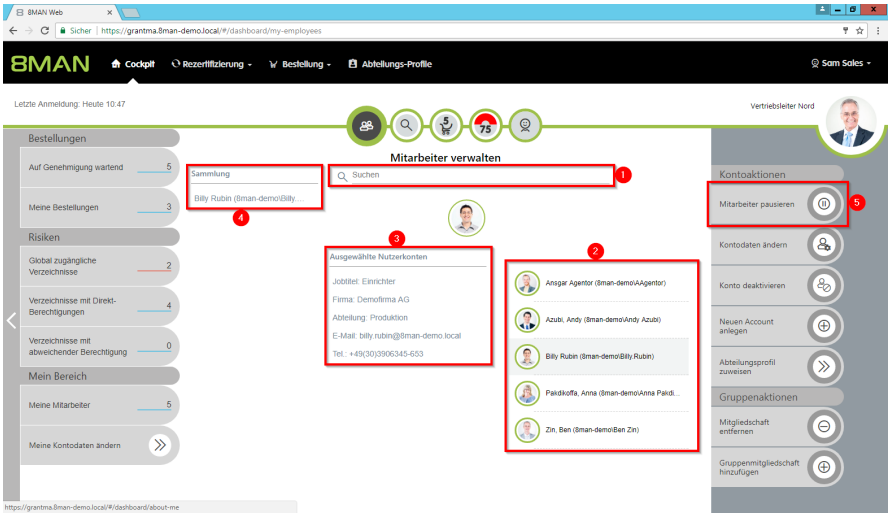
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

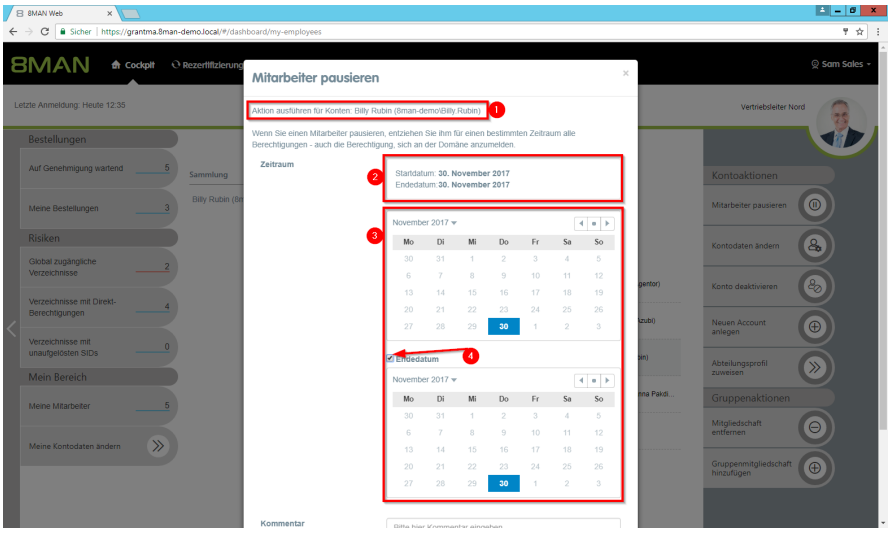


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

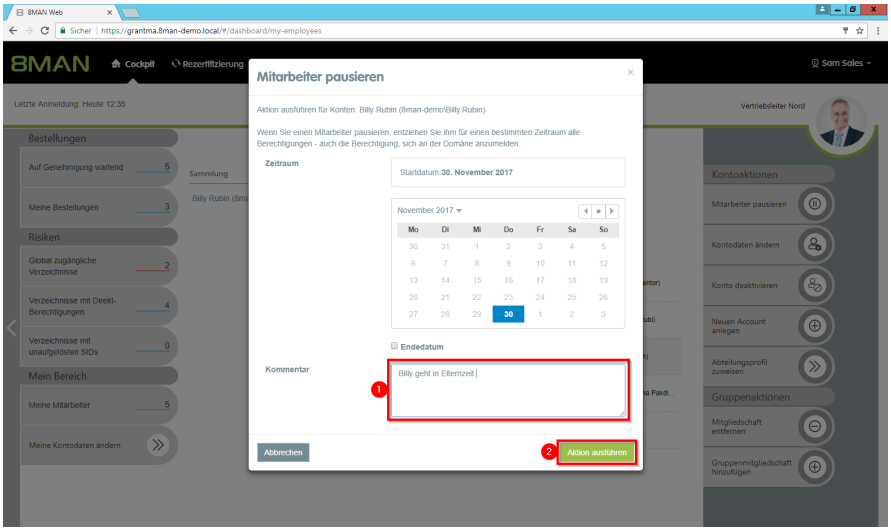
Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Konten zu suchen.*
2. *Wählen Sie einen oder mehrere Mitarbeiter/Konten.*
3. *8MAN zeigt Ihnen die Informationen (Attribute) des ausgewählten Kontos. Haben Sie mehrere Konten ausgewählt, werden Ihnen nur die gemeinsamen Attribute angezeigt.*
4. *In der Sammlung sehen Sie bereits ausgewählte Konten.*
5. *Klicken Sie auf "Mitarbeiter pausieren".*



1. *8MAN zeigt Ihnen, welche Konten Sie ausgewählt haben und pausieren wollen.*
2. *8MAN zeigt das Start- und Endedatum.*
3. *Wählen Sie den Beginn und das Ende der Pause.*
4. *Ist die Pause unbefristet, deaktivieren Sie die Option "Endedatum".*



1. *Sie müssen einen Kommentar angeben.*
2. *Klicken Sie auf "Aktion ausführen".*

8.1.3.5 Einen neuen Benutzer anlegen (Cockpit)

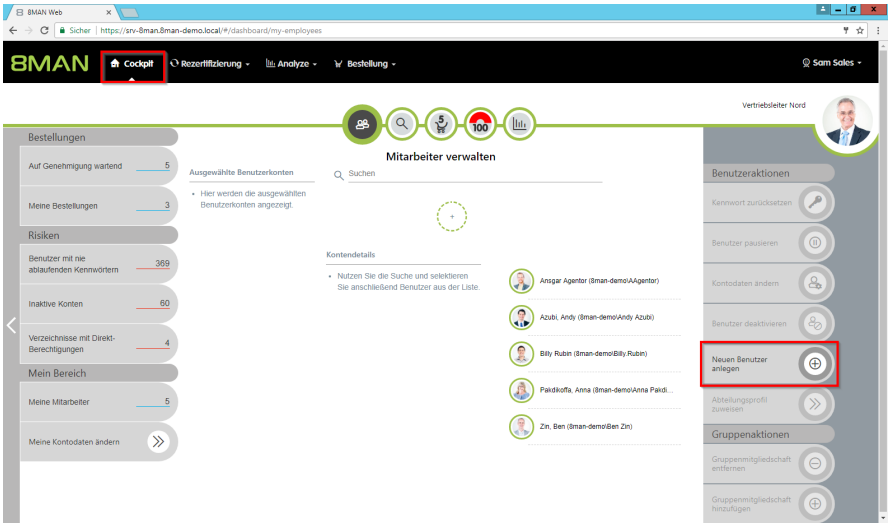
Hintergrund / Mehrwert

Legen Sie im Webclient einen neuen Benutzer an. Die Neuanlage basiert auf von Administratoren vordefinierten Templates und erfolgt deshalb effizient und standardisiert.

Weiterführende Services

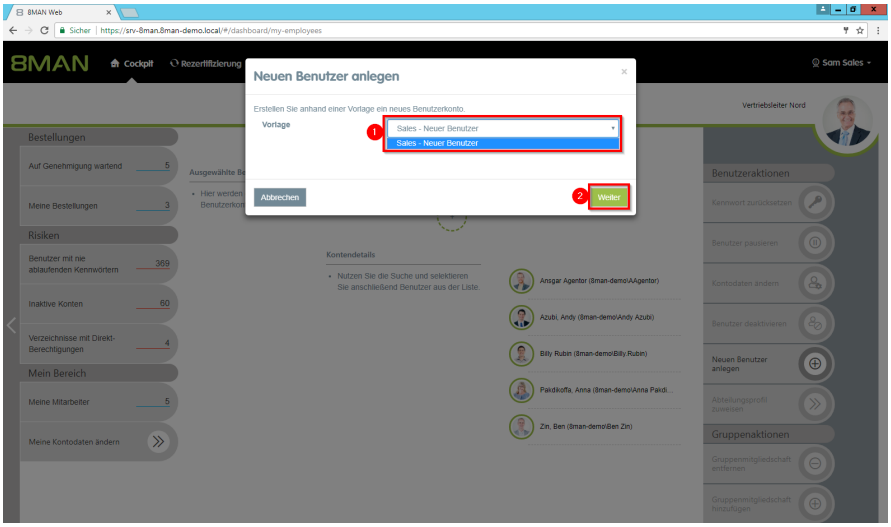
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

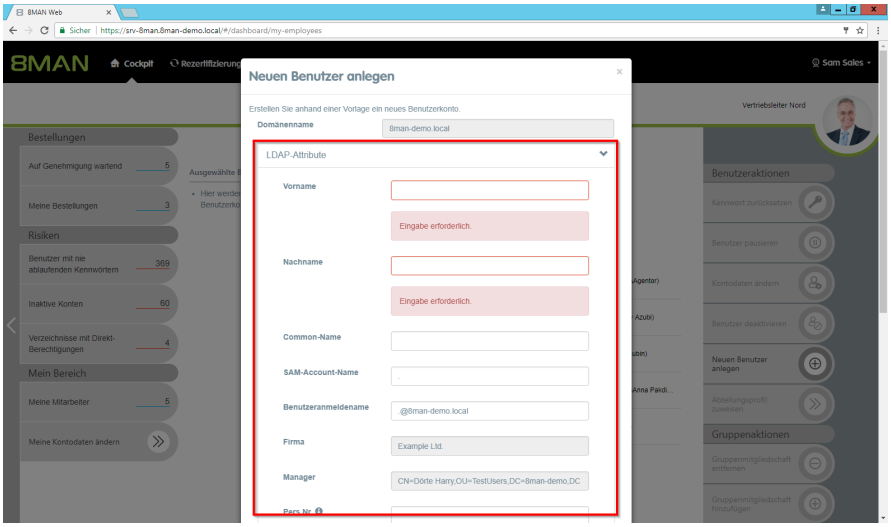


1. *Klicken Sie im Cockpit auf "Neuen Benutzer anlegen".*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.

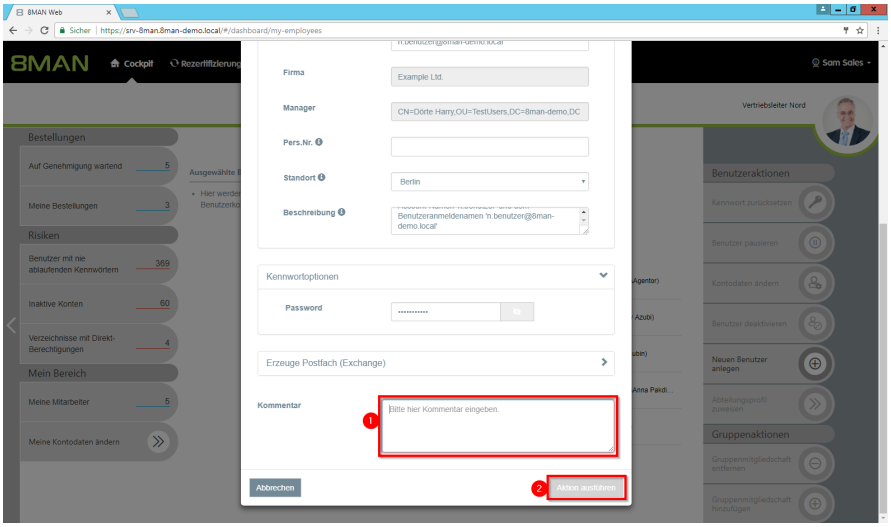


1. *Wählen Sie eine Vorlage aus.*
2. *Klicken Sie auf "Weiter".*



Geben Sie die geforderten Informationen ein.

Der Umfang der hier geforderten Informationen kann stark variieren. Benutzer-Templates müssen von einem Administrator erstellt werden.



1. *Sie müssen einen Kommentar eingeben.*
2. *Klicken Sie auf "Aktion ausführen".*

8.1.3.6 Benutzern ein Abteilungsprofil zuweisen (Cockpit)

Hintergrund / Mehrwert

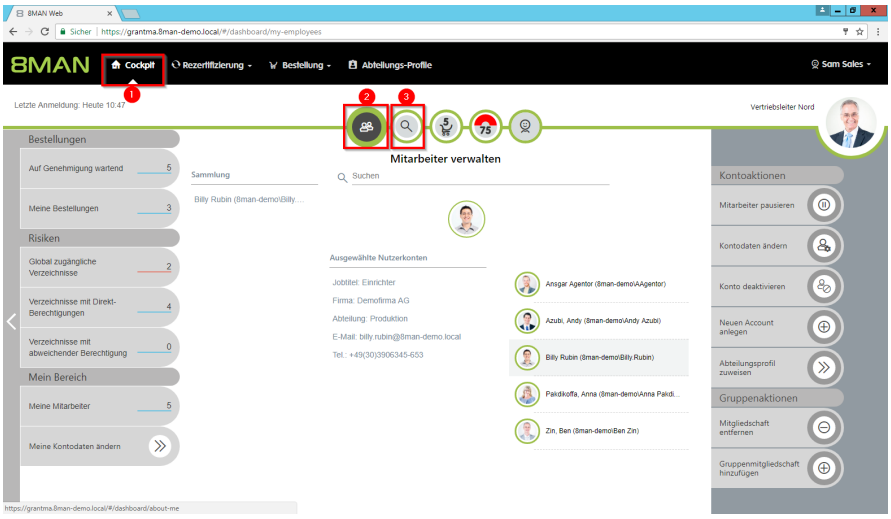
Mit einem Abteilungsprofil weisen Sie einem Benutzer einen Basissatz an Berechtigungen zu. Wechselt der Mitarbeiter die Abteilung, kann der Vorgesetzte einfach ein Abteilungsprofil anwenden. Die alten Berechtigungen können dabei gleich entfernt werden.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle sowie M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements.

Weiterführende Services

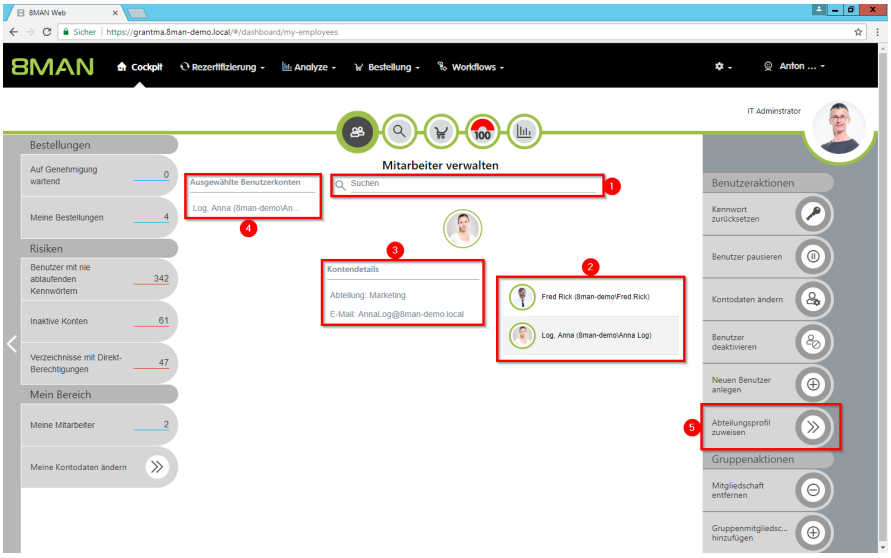
Ein neues Abteilungsprofil erstellen
Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check)

Der Prozess in einzelnen Schritten

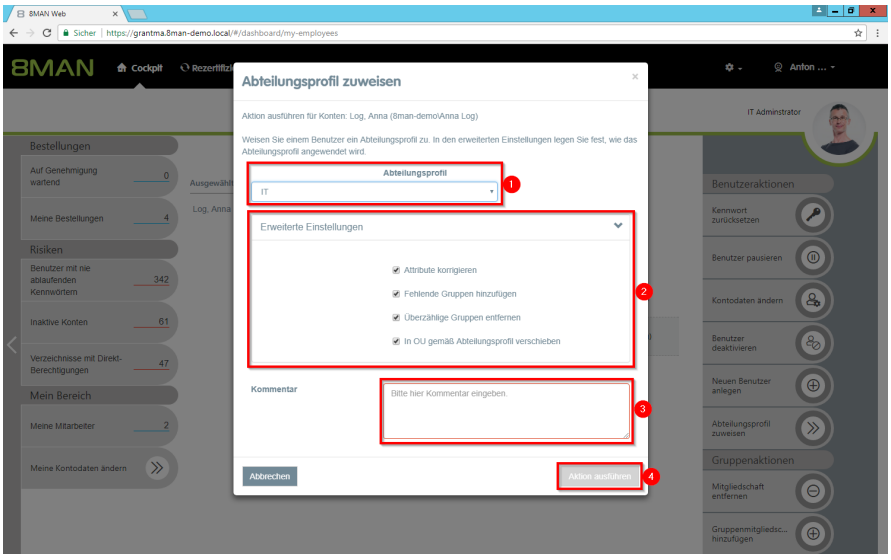


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Konten zu suchen.*
2. *Wählen Sie einen oder mehrere Mitarbeiter/Konten.*
3. *8MAN zeigt Ihnen die Informationen (Attribute) des ausgewählten Kontos. Haben Sie mehrere Konten ausgewählt, werden Ihnen nur die gemeinsamen Attribute angezeigt.*
4. *In der Sammlung sehen Sie bereits ausgewählte Konten.*
5. *Klicken Sie auf "Abteilungsprofil zuweisen".*



1. *Wählen Sie ein Abteilungsprofil.*
2. *Legen Sie in den erweiterten Einstellungen fest, wie das Abteilungsprofil angewendet wird.*
3. *Sie müssen einen Kommentar eingeben.*
4. *Klicken Sie auf "Aktion ausführen".*

8.1.3.7 Die eigenen Kontodaten ändern (Cockpit)

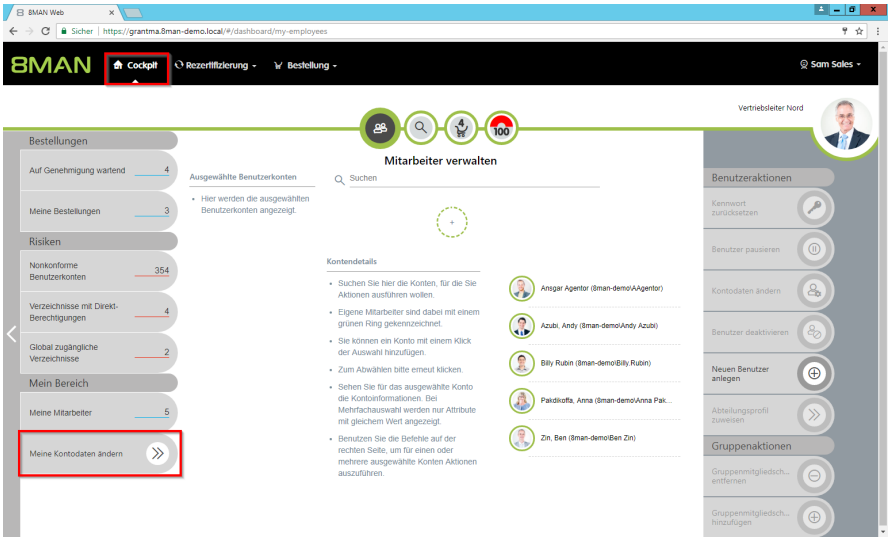
Hintergrund / Mehrwert

Mit 8MAN können Sie schnell und komfortabel die eigenen Kontoinformationen ändern. Die Aktionen werden für die Revision dokumentiert.

Weiterführende Services

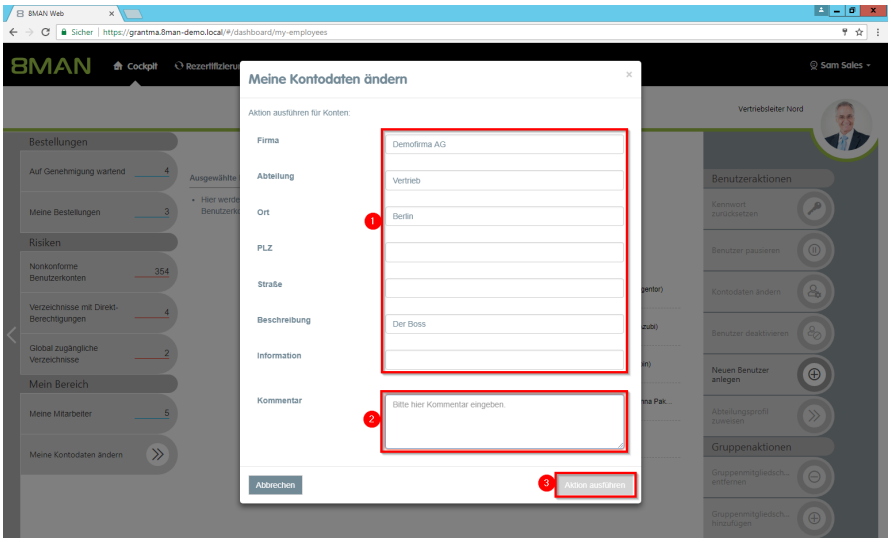
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten



Klicken Sie im Cockpit auf "Meine Kontodaten ändern".

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Ändern Sie Ihre Kontoinformationen.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Klicken Sie auf "Aktion ausführen".*

Die in dem Dialog angezeigten Attribute können von einem Administrator angepasst werden. Dazu muss eine Anpassung der Konfigurationsdatei vorgenommen werden. Eine Anleitung finden Sie in unserer Knowledgebase (Login erforderlich).

8.1.3.8 Meine Mitarbeiter verwalten (Cockpit)

Hintergrund / Mehrwert

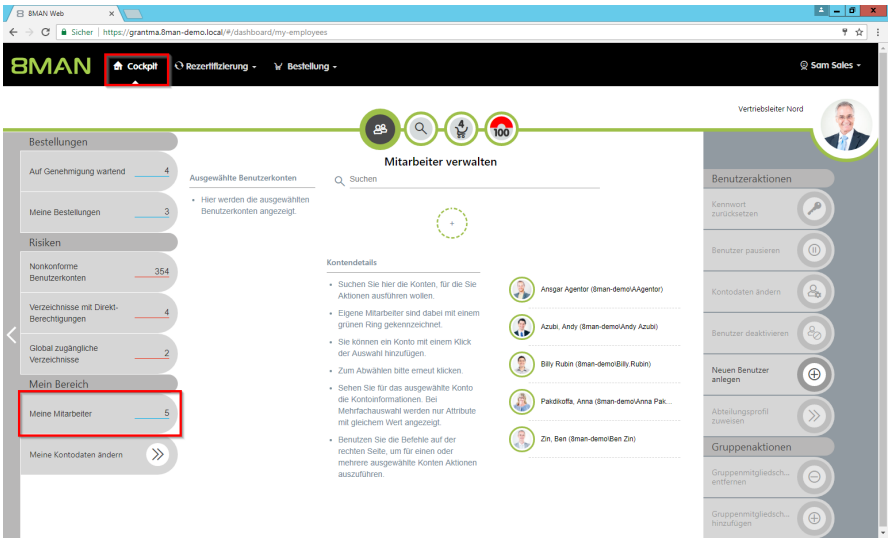
Mit 8MAN können Sie schnell und komfortabel die Ihnen zugeordneten Mitarbeiter verwalten. Aktionen werden für die Revision dokumentiert.

Mitarbeiter sind Benutzer, bei denen Sie als "Vorgesetzter" im Active Directory eingetragen sind. Fragen Sie dazu Ihren Administrator.

Weiterführende Services

Übersicht aller Cockpit-Services

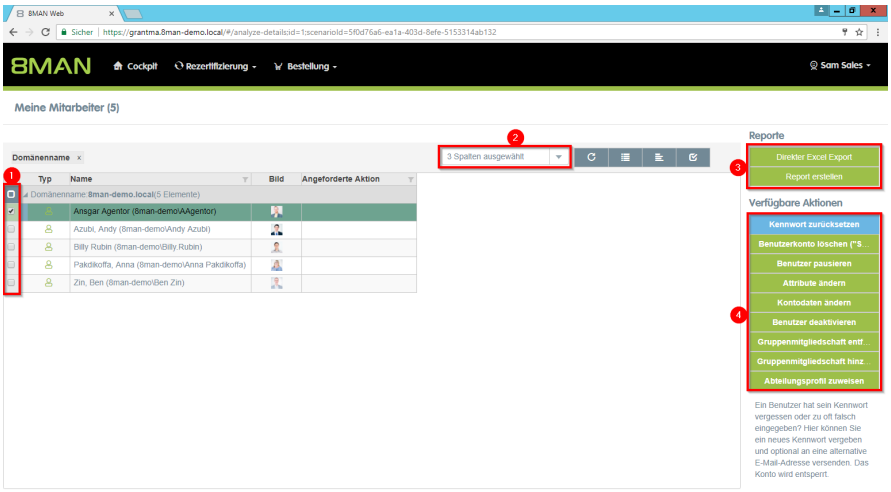
Der Prozess in einzelnen Schritten



Klicken Sie im Cockpit auf "Meine Mitarbeiter".

Die Schaltfläche zeigt Ihnen, wieviele Mitarbeiter Ihnen zugeordnet sind.

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Selektieren Sie Mitarbeiter.*
2. *Passen Sie an, welche Spalten angezeigt werden.*
3. *Exportieren Sie die Liste zu Excel oder PDF.*
4. *Führen Sie Aktionen auf den ausgewählten Mitarbeiterkonten aus.*

8.1.3.9 Gruppenmitgliedschaften hinzufügen (Cockpit)

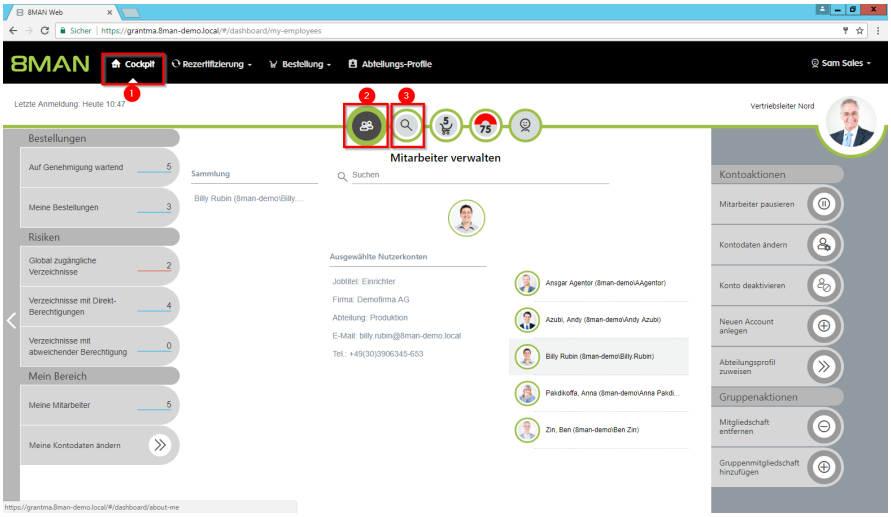
Hintergrund / Mehrwert

Stellt z. B. ein Manager fest, dass seinem Mitarbeiter eine Gruppenmitgliedschaft fehlt, kann er diese in wenigen einfachen Schritten hinzufügen.

Weiterführende Services

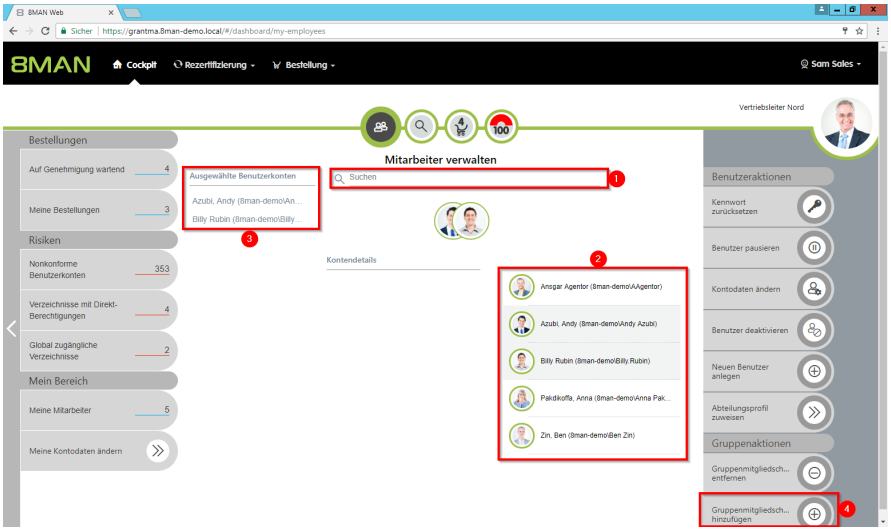
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

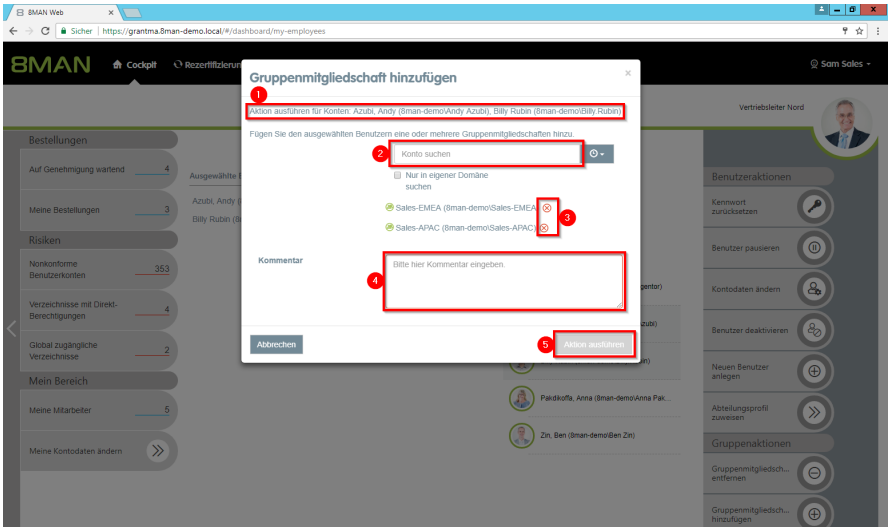


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Konten zu suchen.*
2. *Wählen Sie einen oder mehrere Mitarbeiter/Konten.*
3. *In der Sammlung sehen Sie bereits ausgewählte Konten.*
4. *Klicken Sie auf "Gruppenmitgliedschaften hinzufügen".*



1. *8MAN zeigt Ihnen, welche Konten Sie ausgewählt haben.*
2. *Suchen Sie nach Gruppen.*
3. *Entfernen Sie bereits ausgewählte Gruppen.*
4. *Sie müssen einen Kommentar angeben.*
5. *Klicken Sie auf "Aktion ausführen".*

8.1.3.10 Gruppenmitgliedschaften entfernen (Cockpit)

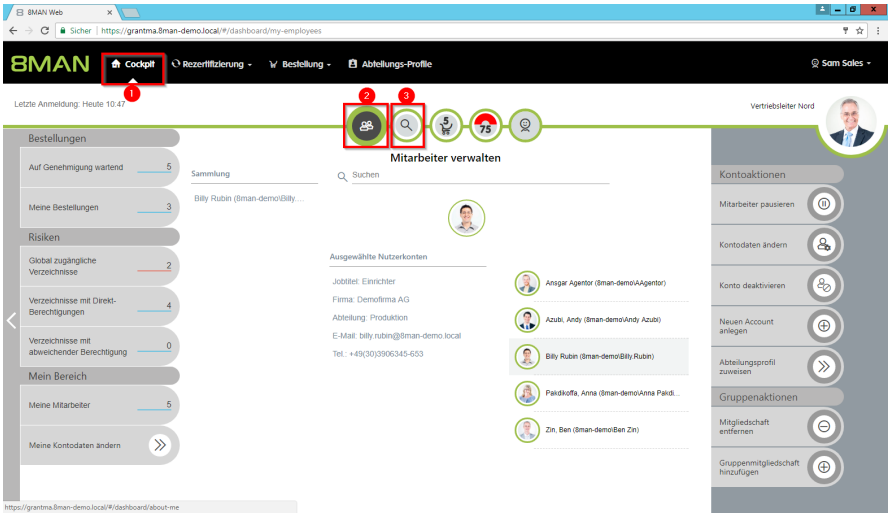
Hintergrund / Mehrwert

Überberechtigungen entstehen häufig durch Gruppenmitgliedschaften. Im Cockpit können Sie schnell Gruppenmitgliedschaften entfernen.

Weiterführende Services

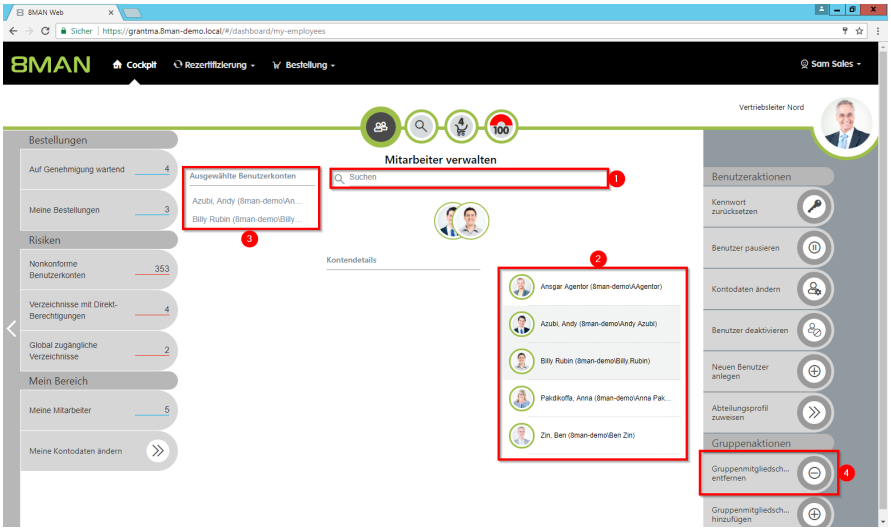
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

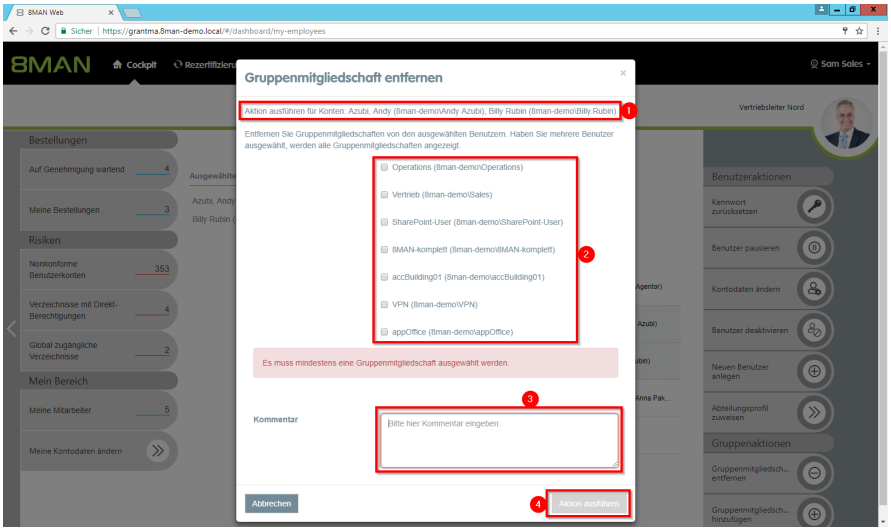


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



1. *Nutzen Sie die Suche, um eine lange Mitarbeiterliste zu filtern oder nach Konten zu suchen.*
2. *Wählen Sie einen oder mehrere Mitarbeiter/Konten.*
3. *In der Sammlung sehen Sie bereits ausgewählte Konten.*
4. *Klicken Sie auf "Gruppenmitgliedschaften entfernen".*



1. *8MAN zeigt Ihnen, welche Konten Sie ausgewählt haben.*
2. *Selektieren Sie mindestens eine Gruppe.*
3. *Sie müssen einen Kommentar angeben.*
4. *Klicken Sie auf "Aktion ausführen".*

8.2 Fileserver

8.2.1 Data Owner

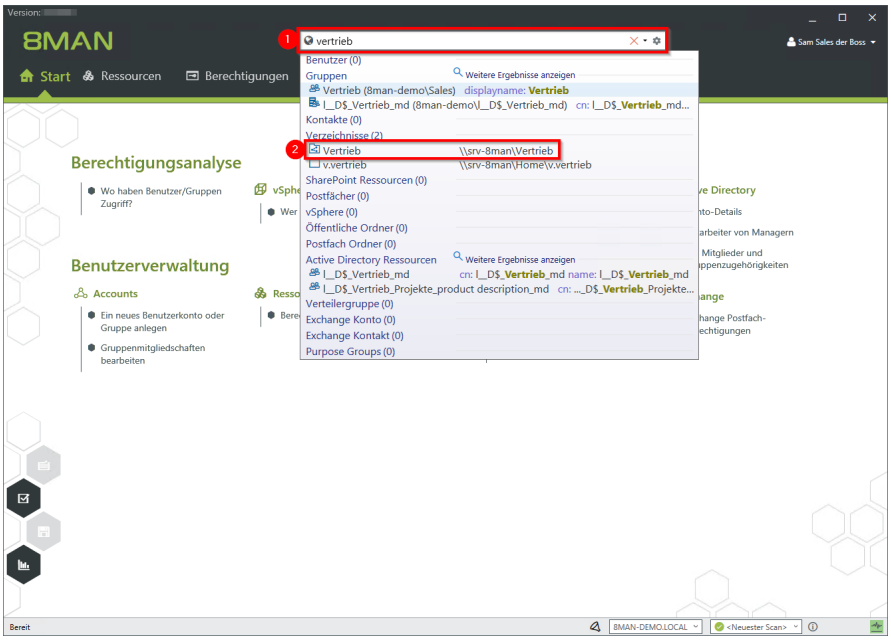
8.2.1.1 Verzeichnisberechtigungen für Mitarbeiter erteilen und entziehen

Hintergrund / Mehrwert

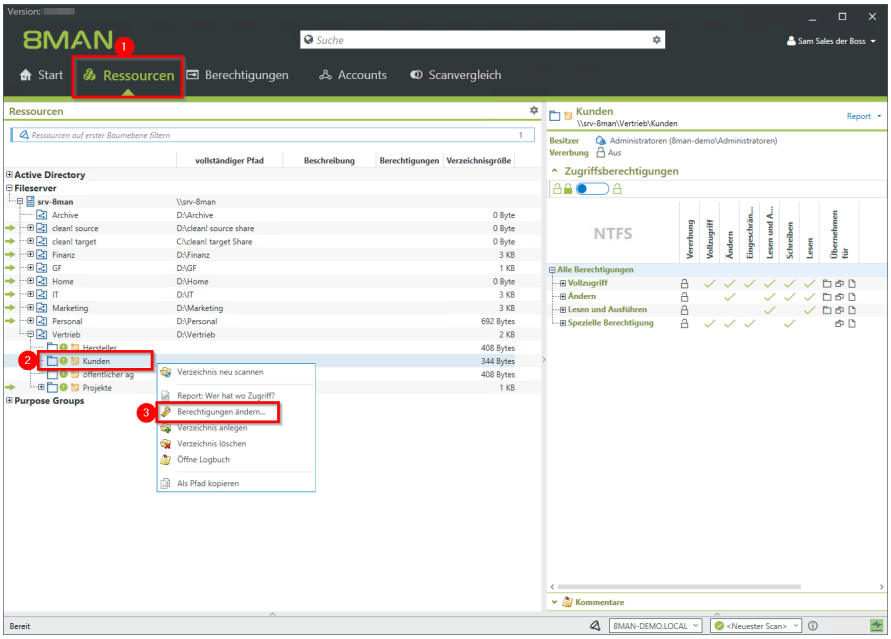
Berechtigungen sollten schnell vergeben und wieder entzogen werden. Deshalb können sie das für Ihre Mitarbeiter selbst erledigen. Sie benötigen keine Fachkenntnisse über Active Directory und Fileserver. Entscheiden Sie einfach, welche Rechte sie vergeben möchten: "Ändern" oder "Lesen und Ausführen".

Für eine bessere Datenintegrität empfehlen wir "Ändern" nur ausgewählten Mitarbeitern zu vergeben.

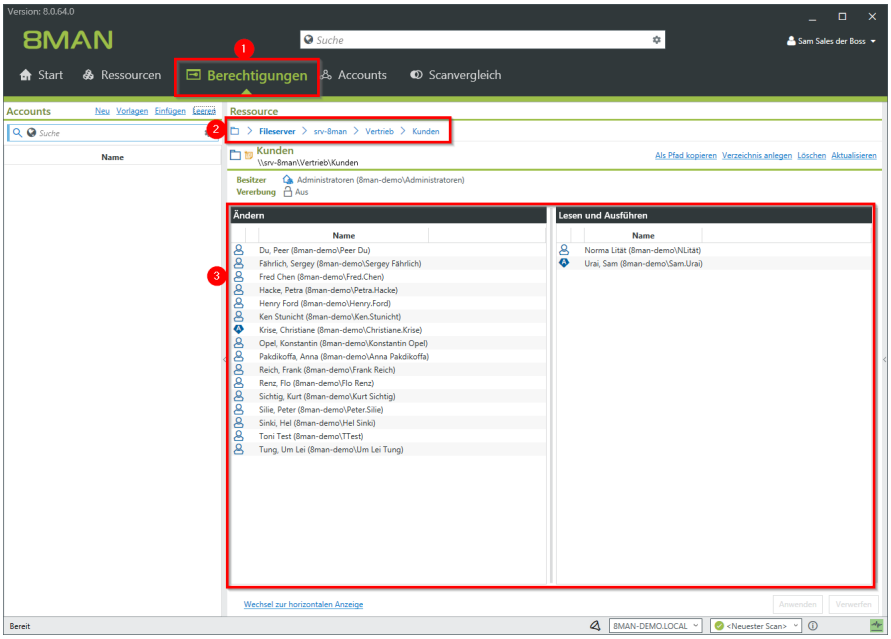
Der Prozess in einzelnen Schritten



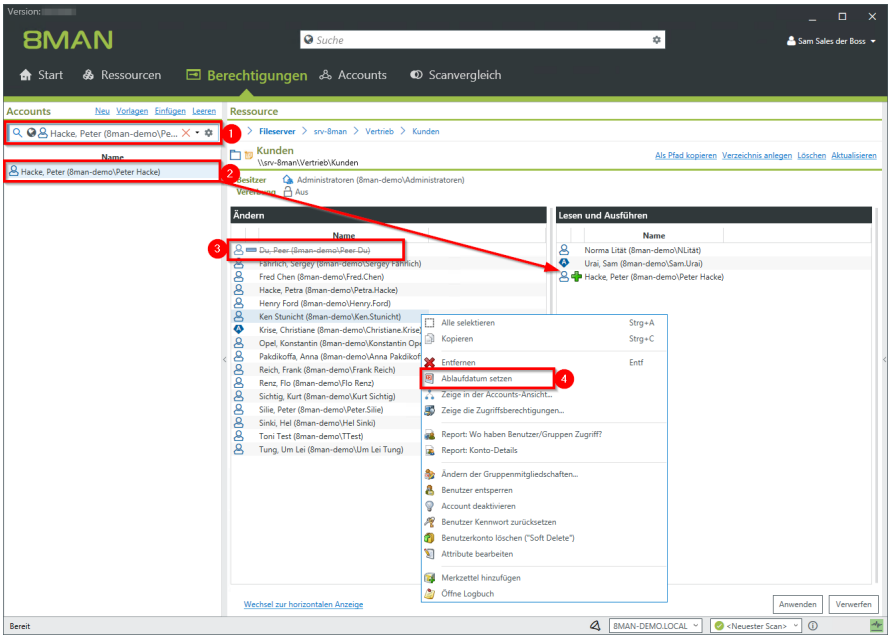
1. *Verwenden Sie die Suche, um das gewünschte Verzeichnis zu finden.*
2. *Klicken Sie auf das Suchergebnis.*



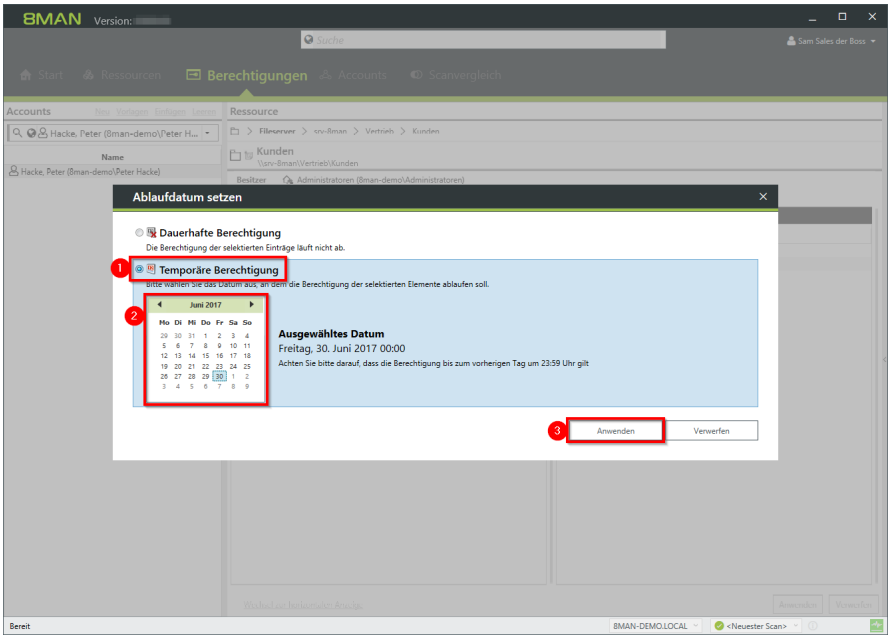
1. *8MAN wechselt in die Ansicht "Ressourcen".*
2. *Wählen Sie ggf. in ein Unterverzeichnis. Rechtsklicken Sie das gewünschte Verzeichnis.*
3. *Klicken Sie auf "Berechtigungen ändern...".*



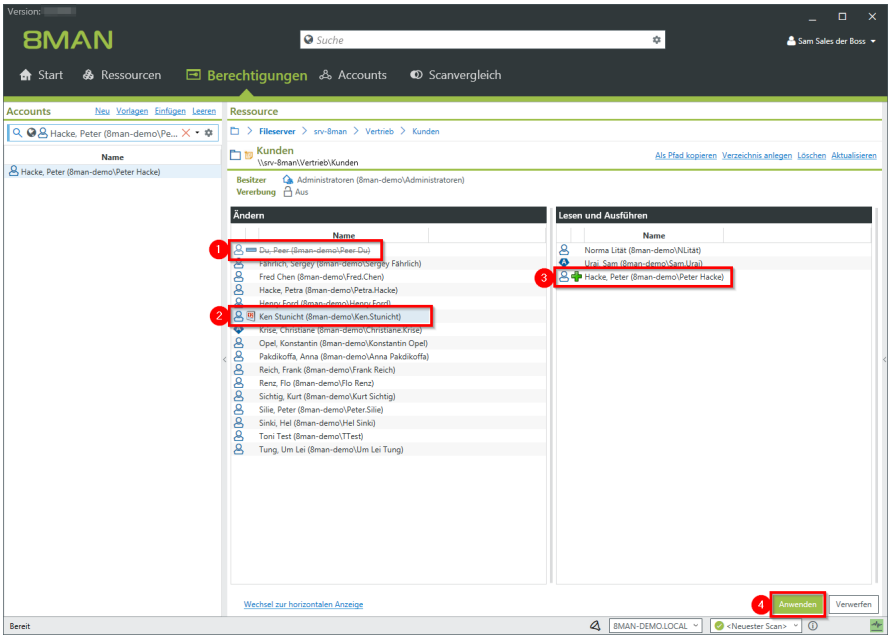
1. *8MAN wechselt in die Ansicht "Berechtigungen".*
2. *8MAN zeigt Ihnen das Verzeichnis, an dem Sie arbeiten. Sie können das Verzeichnis wechseln.*
3. *8MAN zeigt Ihnen die bestehenden Berechtigungen in den Zugriffskategorien "Ändern" und "Lesen und Ausführen".*



1. *Finden Sie mit der Suche einen Benutzer oder eine Gruppe.*
2. *Ziehen Sie Benutzer per Drag&Drop auf eine Spalte, um eine Berechtigung zuzuweisen.*
3. *Klicken Sie mit der rechten Maustaste auf einen Eintrag, um eine Berechtigung zu entziehen - sofort oder zu einem geplanten Zeitpunkt. Klicken Sie auf "Ablaufdatum setzen".*

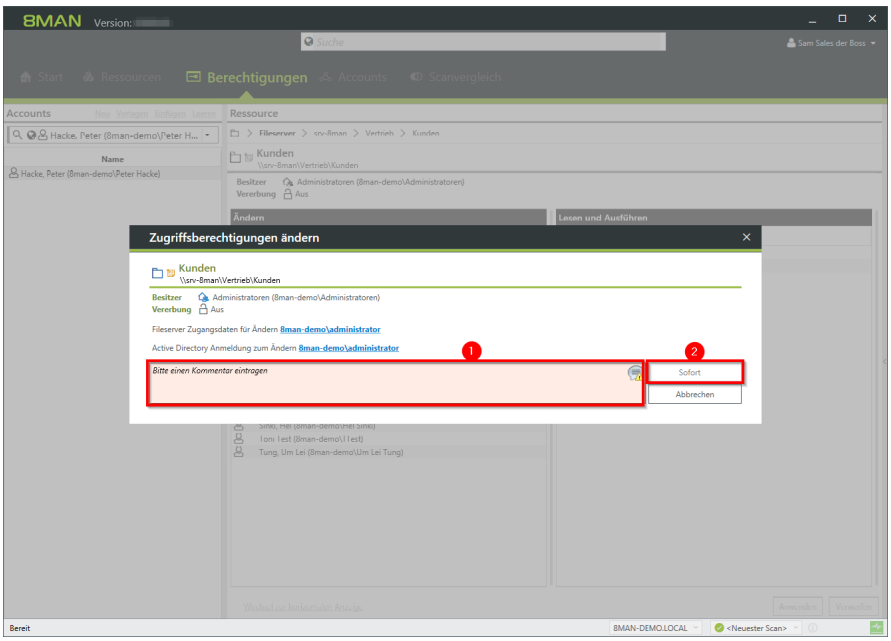


1. *Aktivieren Sie die Option "Temporäre Berechtigung".*
2. *Setzen Sie ein Ablaufdatum.*
3. *Klicken Sie auf "Anwenden".*



8MAN zeigt alle geplanten Berechtigungsänderungen:

1. *Eine Berechtigung entziehen.*
2. *Ein Ablaufdatum für eine Berechtigung setzen.*
3. *Eine Berechtigung erteilen.*
4. *Klicken Sie auf "Anwenden".*



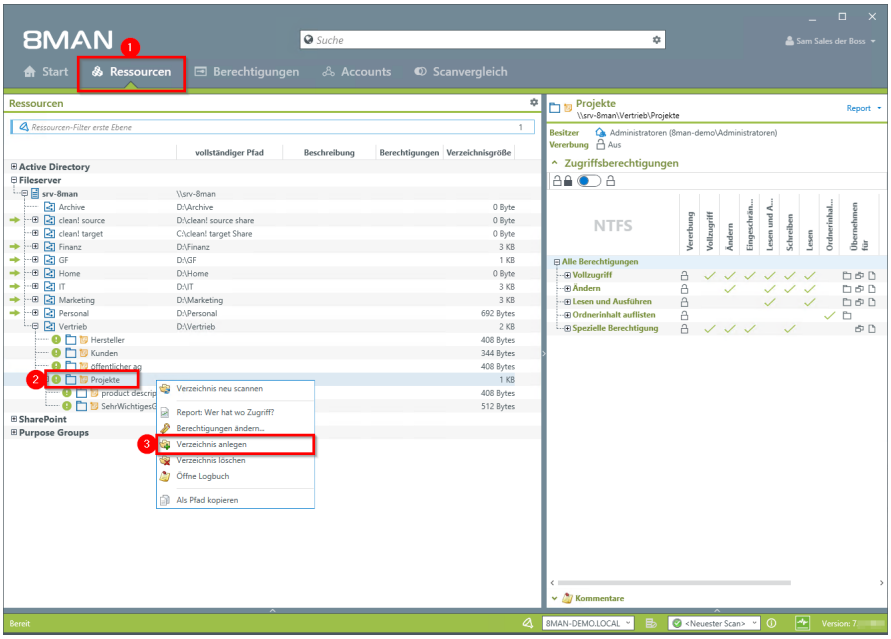
1. *Sie müssen einen Kommentar eingeben.*
2. *Starten Sie die Berechtigungsänderung.*

8.2.1.2 Einen geschützten Fileserverbereich anlegen

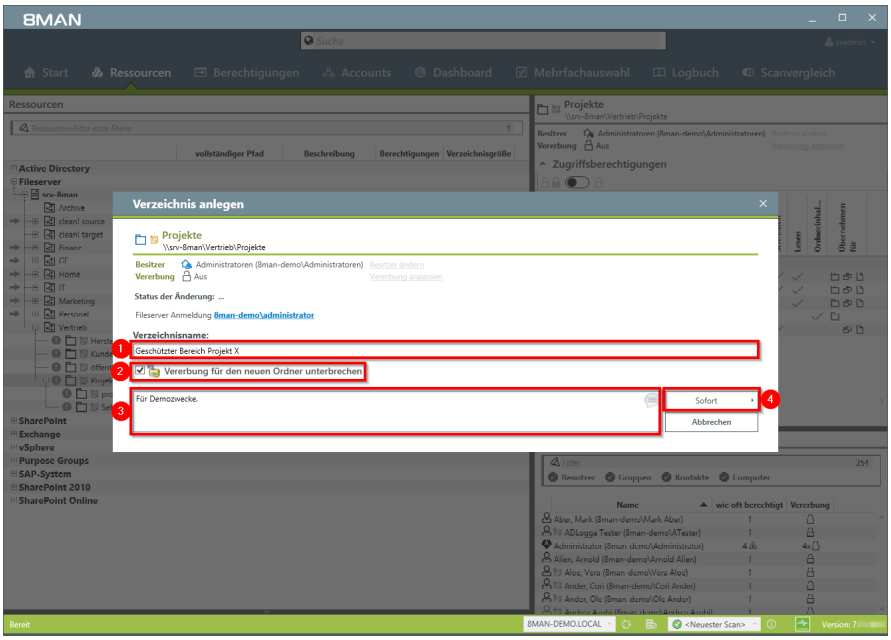
Hintergrund / Mehrwert

Führungskräfte können mit 8MAN blitzschnell geschützte Fileserverbereiche anlegen. Dazu wird mit 8MAN ein Verzeichnis erstellt, die automatisch vererbten Berechtigungen entfernt und anschliessend neue Berechtigungen vergeben. Das Resultat ist ein geschützter Arbeitsbereich, auf den nur ausgewählte Mitglieder Zugriff haben.

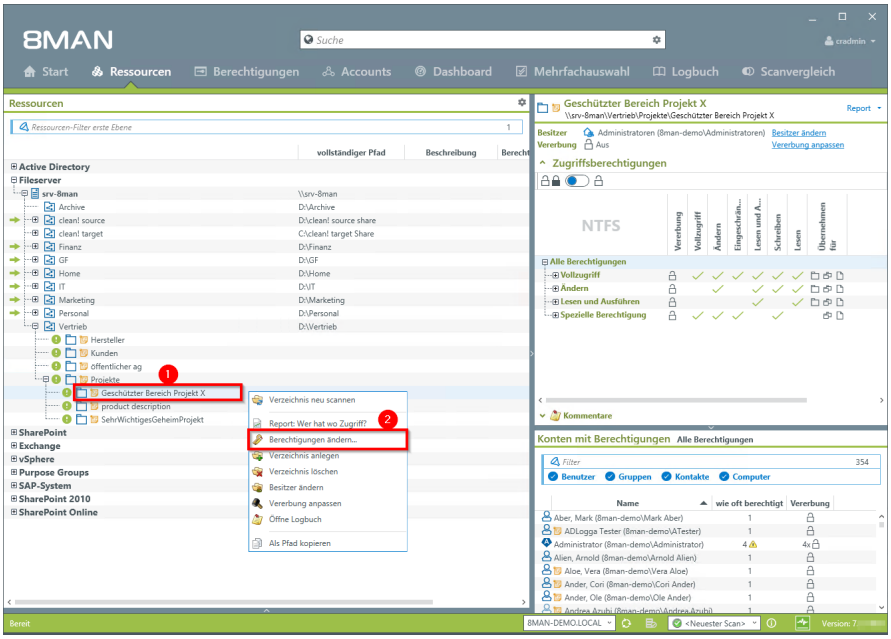
Der Prozess in einzelnen Schritten



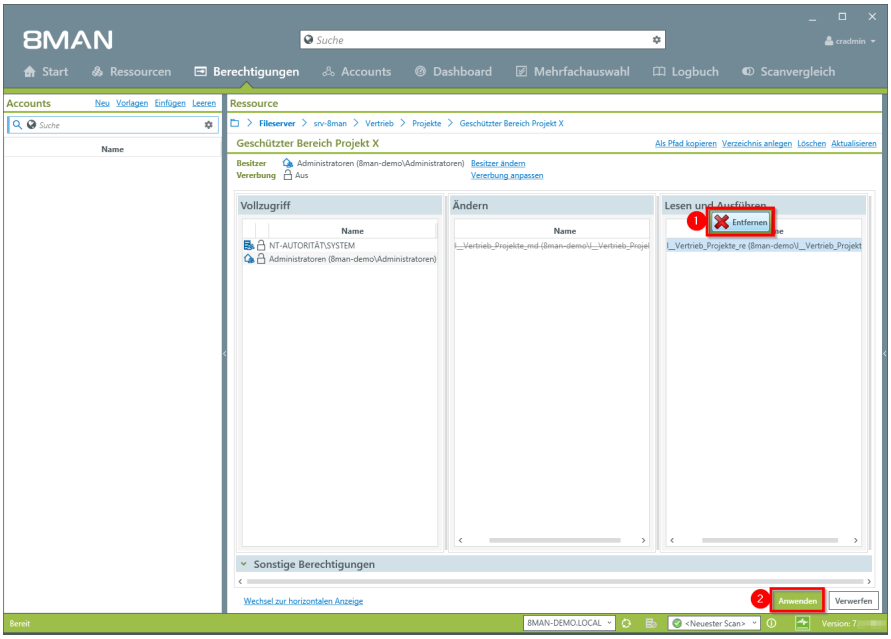
1. *Wählen Sie "Ressourcen".*
2. *Navigieren Sie zum gewünschten Ordner.*
3. *Rechtsklicken Sie den Ordner und wählen "Verzeichnis anlegen" im Kontextmenü.*



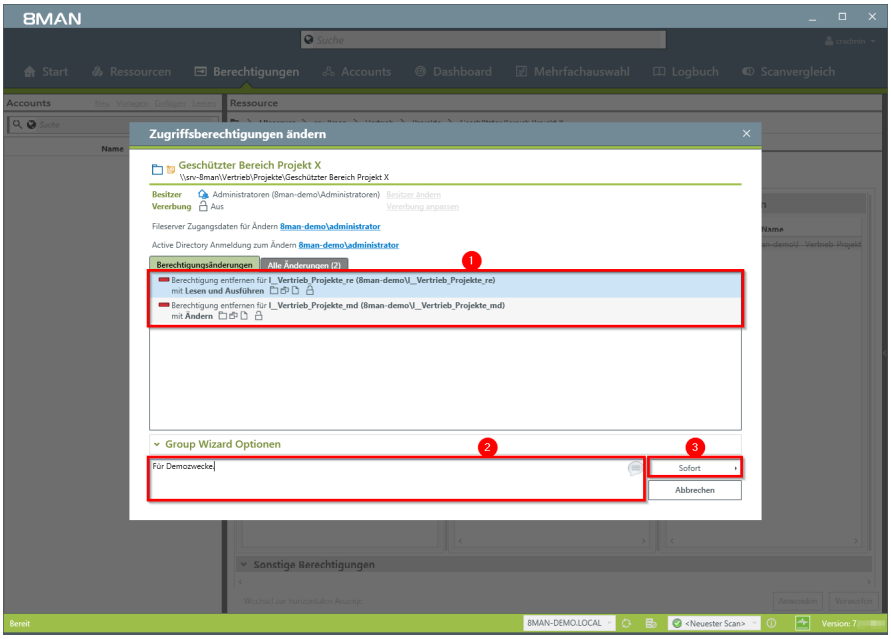
1. *Geben Sie dem Verzeichnis einen Namen.*
2. *Aktivieren Sie die Option.*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie das Erstellen des neuen Bereichs.*



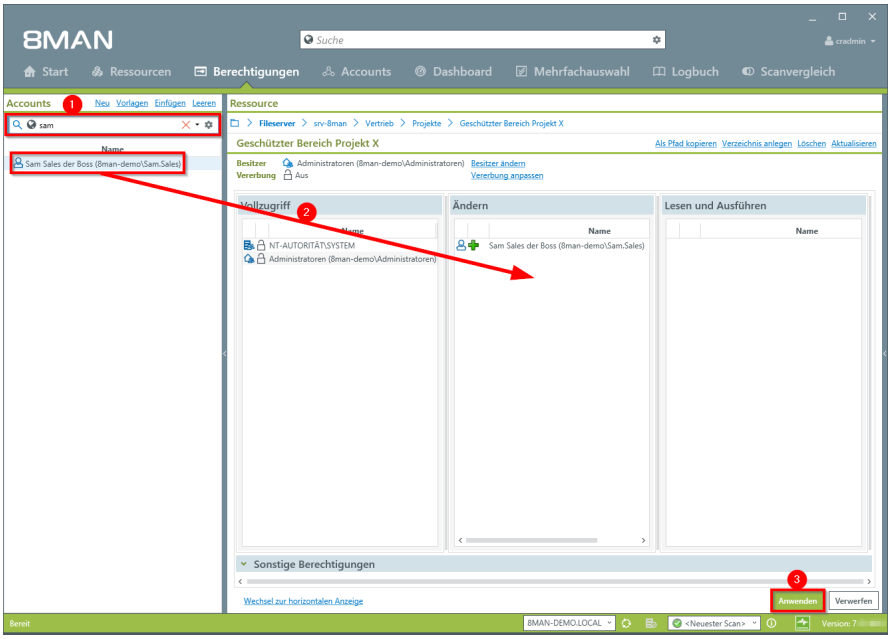
1. *Navigieren Sie zum neu erstellten Verzeichnis.*
2. *Rechtsklicken Sie das Verzeichnis und wählen "Berechtigungen ändern..." im Kontextmenü.*



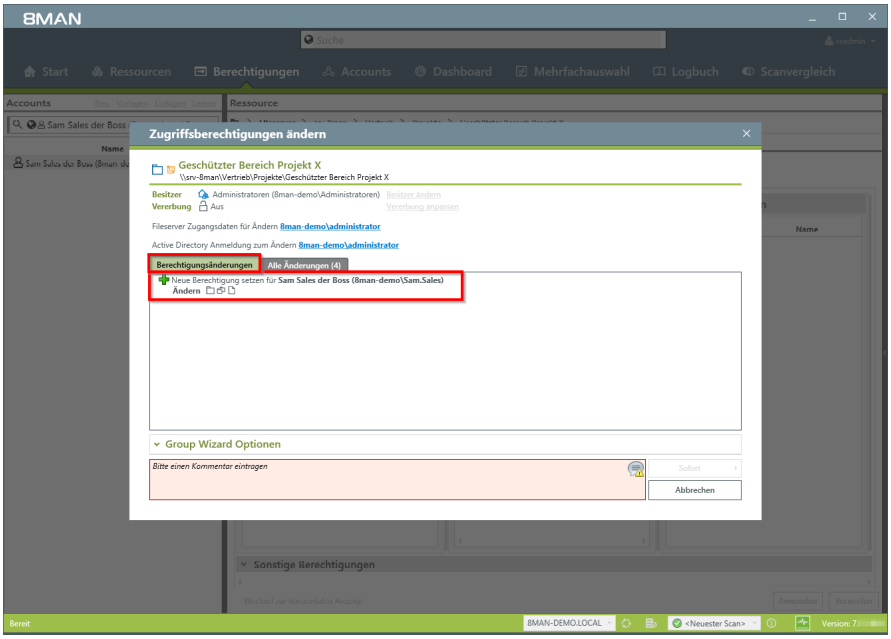
1. *Löschen Sie alle nicht benötigten Berechtigungen.*
2. *Klicken Sie auf "Anwenden".*



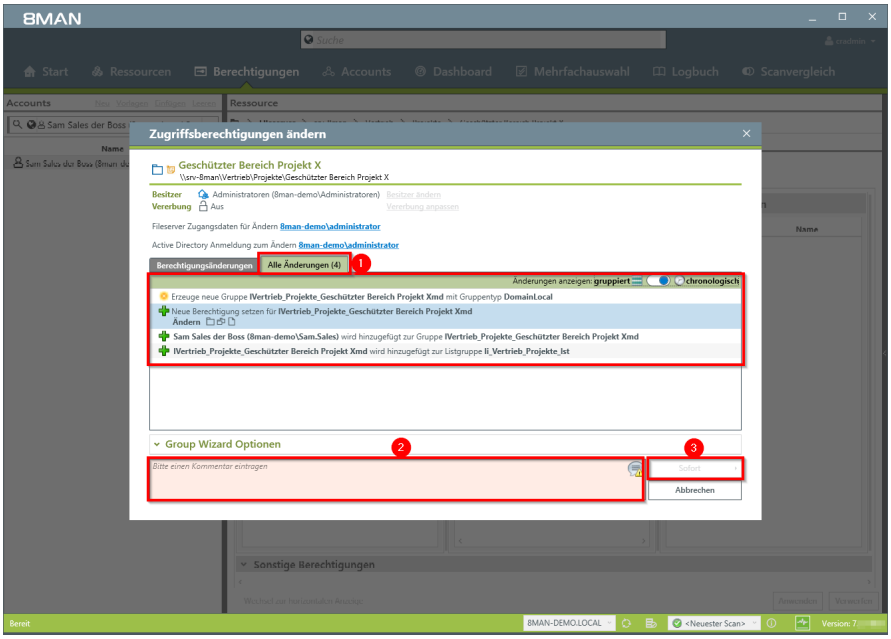
1. *8MAN listet die geplanten Berechtigungsänderungen auf.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie die Änderung.*



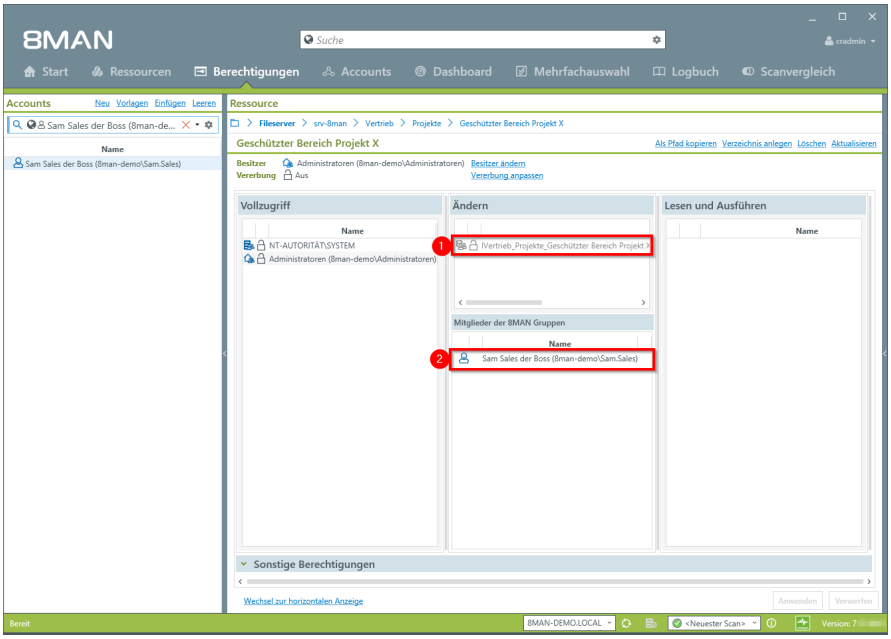
1. *Nutzen Sie die Suchfunktion, um Gruppen oder Benutzer zu finden.*
2. *Ziehen Sie per Drag&Drop die gewünschten Accounts auf die Zugriffskategorie-Spalten.*
3. *Starten Sie die Änderung.*



8MAN listet die geplante Berechtigungsänderung auf. In dem gezeigten Beispiel erhält "Sam Sales" das "Ändern"-Recht auf dem neuen geschützten Bereich.



1. *Klicken Sie auf den Reiter "Alle Änderungen". Sie sehen alle Schritte, die der Group Wizard in diesem Beispiel ausführt.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie die Änderung.*



Nach der Ausführung zeigt Ihnen 8MAN das Ergebnis:

1. *Eine nach Bildungsvorschrift automatisch neu erstellte 8MAN-Gruppe für das Ändern-Recht.*
2. *Sam Sales, der Mitglied der neuen Gruppe geworden ist.*

8.2.2 Administrator

8.2.2.1 Mehrfachberechtigungen auf Verzeichnissen entfernen

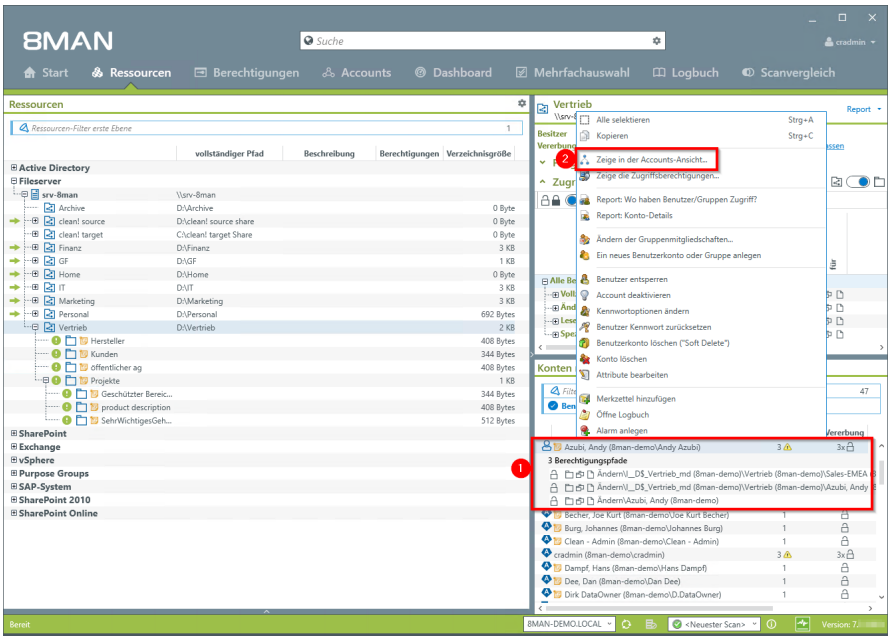
Hintergrund / Mehrwert

Mehrfachberechtigungen kommen über die Mitgliedschaft mit verschachtelten Gruppen im AD zustande. Sie sind Ausdruck einer unsauberen Gruppenstruktur. Denn: Eine Berechtigung sollte sich nur aus einer Gruppenmitgliedschaft ergeben. Mit 8MAN können Sie Mehrfachberechtigungen schnell entfernen.

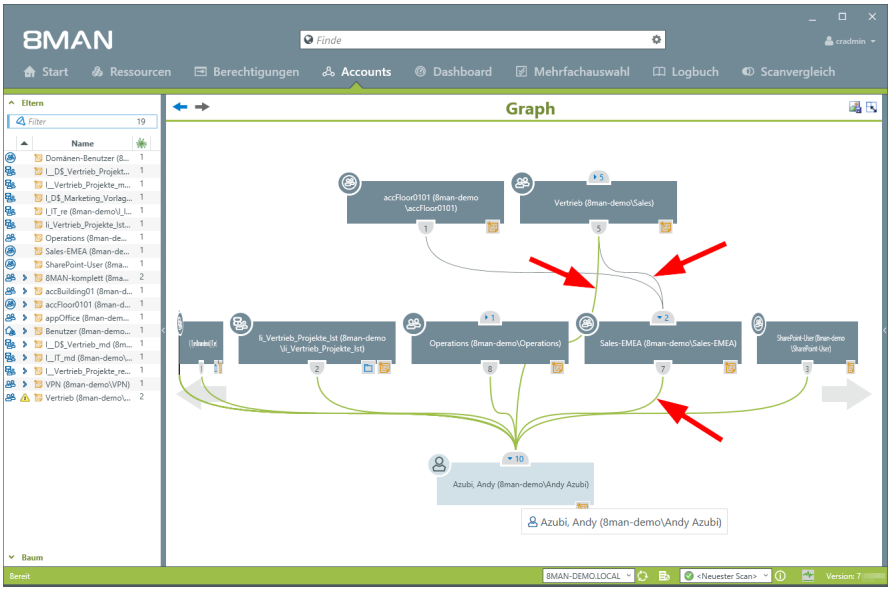
Weiterführende Services

Mehrfachberechtigungen auf Verzeichnissen identifizieren

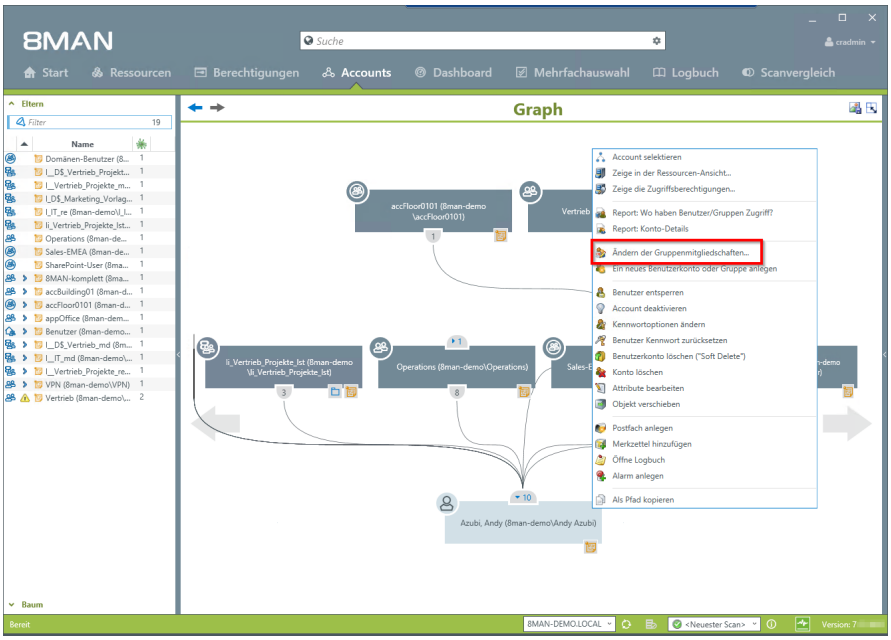
Der Prozess in einzelnen Schritten



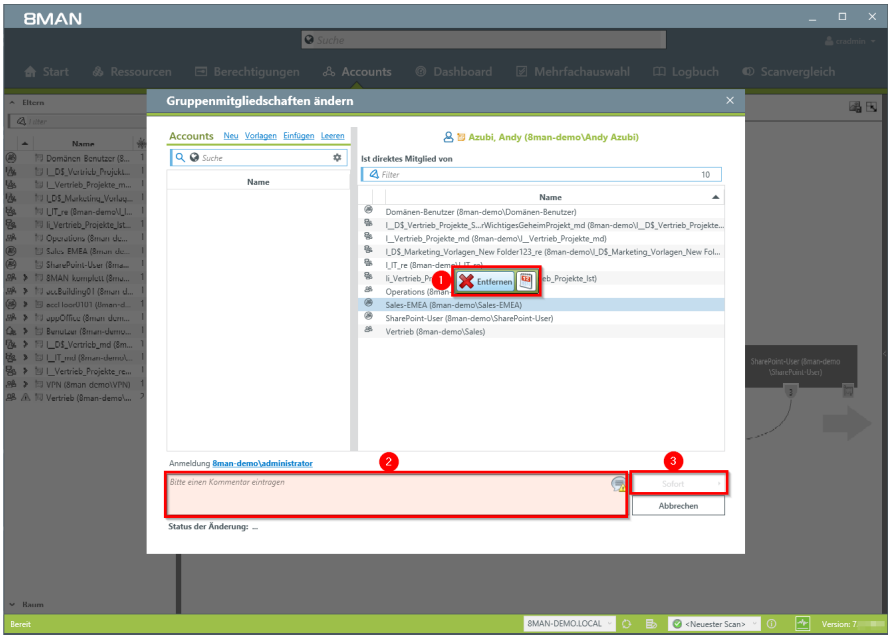
1. *Sie haben für "Andy Azubi" Mehrfachberechtigungen identifiziert.*
2. *Rechtsklicken Sie auf den Account und wählen "Zeige in der Accounts-Ansicht..." im Kontextmenü.*



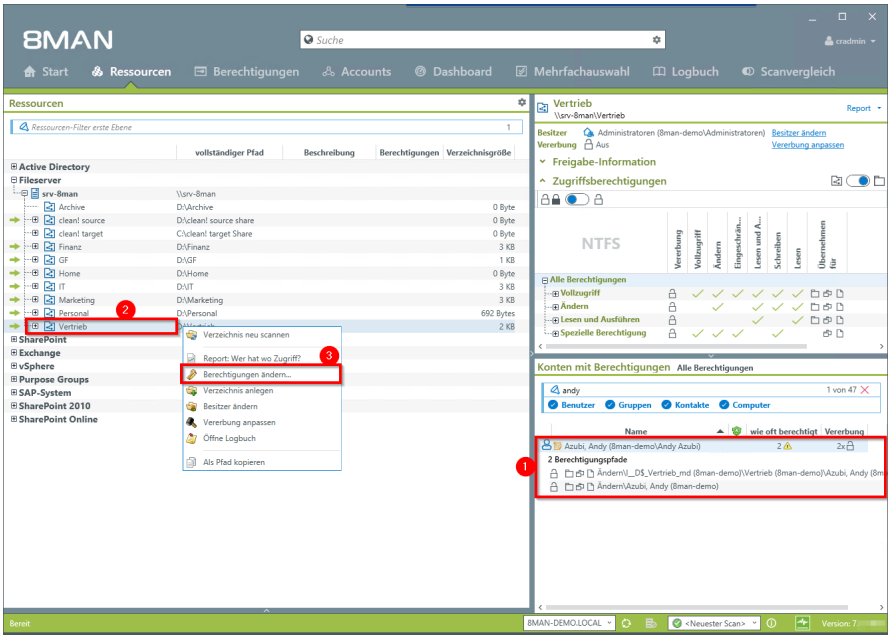
Analysieren Sie mit dem Account-Graphen, wie die Mehrfachberechtigungen aufgebaut sind.



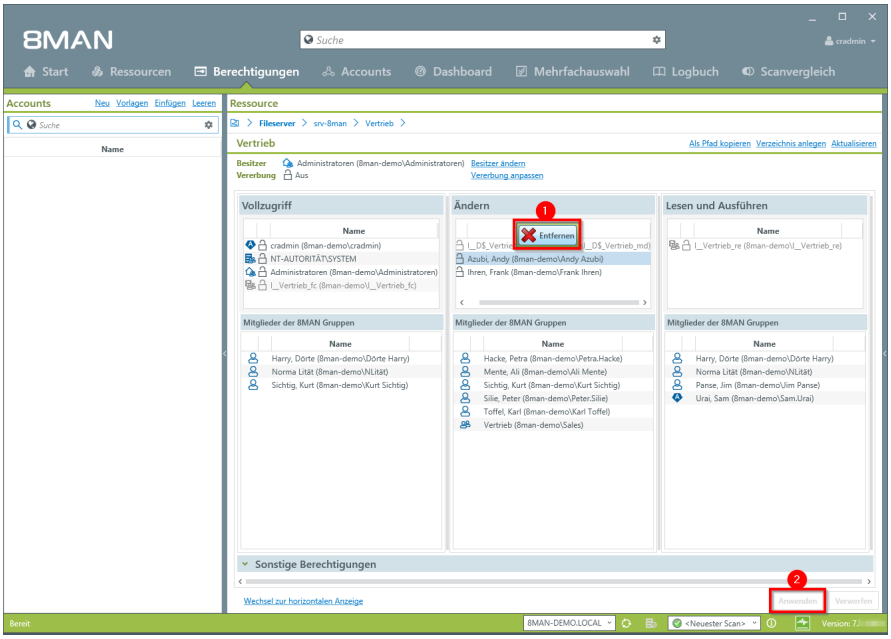
Rechtsklicken Sie den Account und wählen "Ändern der Gruppenmitgliedschaften..." im Kontextmenü.



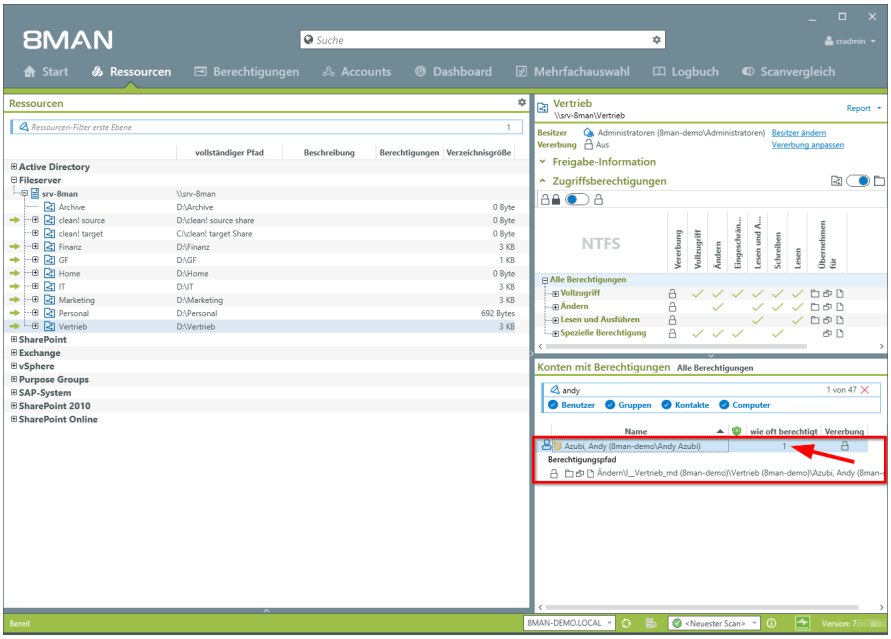
1. *Entfernen Sie die Gruppenmitgliedschaft.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie die Ausführung.*



1. *Nach dem Entfernen der überflüssigen Gruppenmitgliedschaften bleibt noch die zusätzliche Direktberechtigung.*
2. *Selektieren Sie das Verzeichnis mit Rechtsklick.*
3. *Wählen Sie im Kontextmenü "Berechtigungen ändern...".*



1. *Selektieren Sie den betreffenden Benutzer und wählen "Entfernen".*
2. *Starten Sie das Entfernen.*



Prüfen Sie das Resultat in der Ressourcenansicht.

8.2.2.2 Direktberechtigungen entfernen

Hintergrund / Mehrwert

Direktberechtigungen sollten unter allen Umständen vermieden werden und durch Berechtigungen über Gruppen ersetzt werden. Direktberechtigungen sind ineffizient, weil jeder Nutzer einzeln berechtigt werden muss. Darüber hinaus muss jedes Verzeichnis bei der Rechteentfernung gesondert geprüft werden. 8MAN zeigt Ihnen alle Direktberechtigungen auf Ihren Fileservern. Anschließend können Sie via Drag & Drop die Direktberechtigung in eine Berechtigung über Gruppen umwandeln.

Weiterführende Services

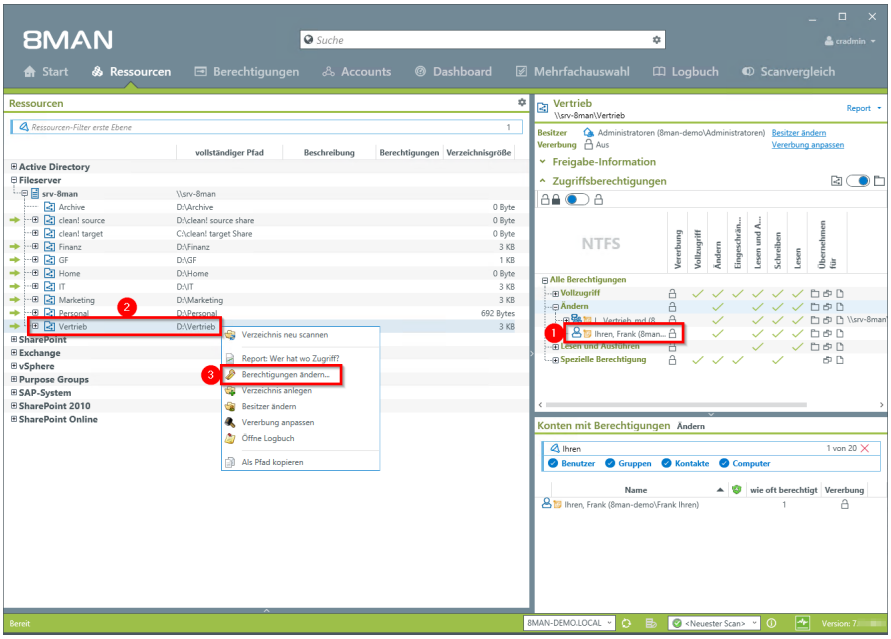
Direktberechtigungen im Bulk entfernen (Webclient)

Mit dem 8MATE Clean! können sie Direktberechtigungen automatisiert entfernen oder umwandeln lassen:

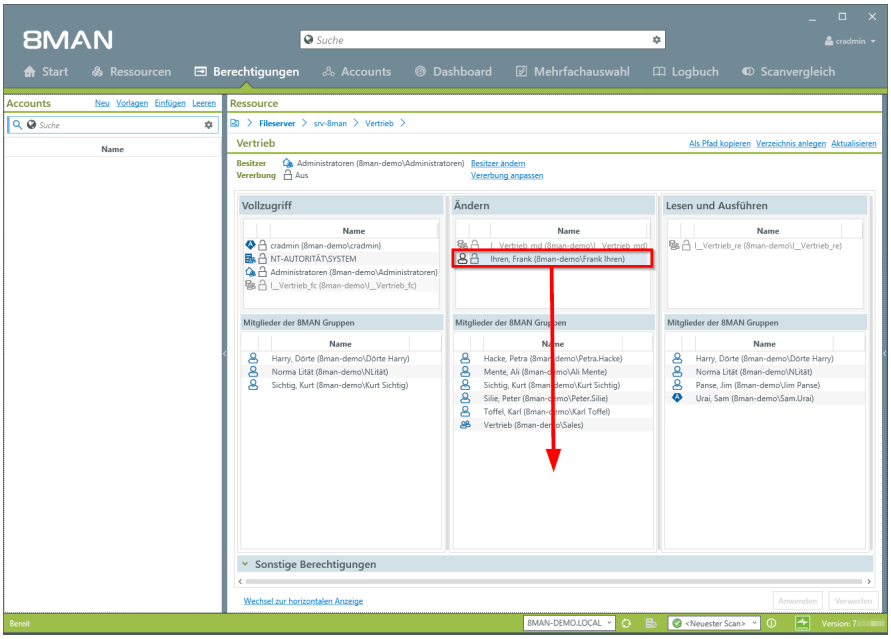
8MATE Clean! Handbuch: Direktberechtigungen löschen

8MATE Clean! Handbuch: Direktberechtigungen durch Gruppenmitgliedschaften ersetzen

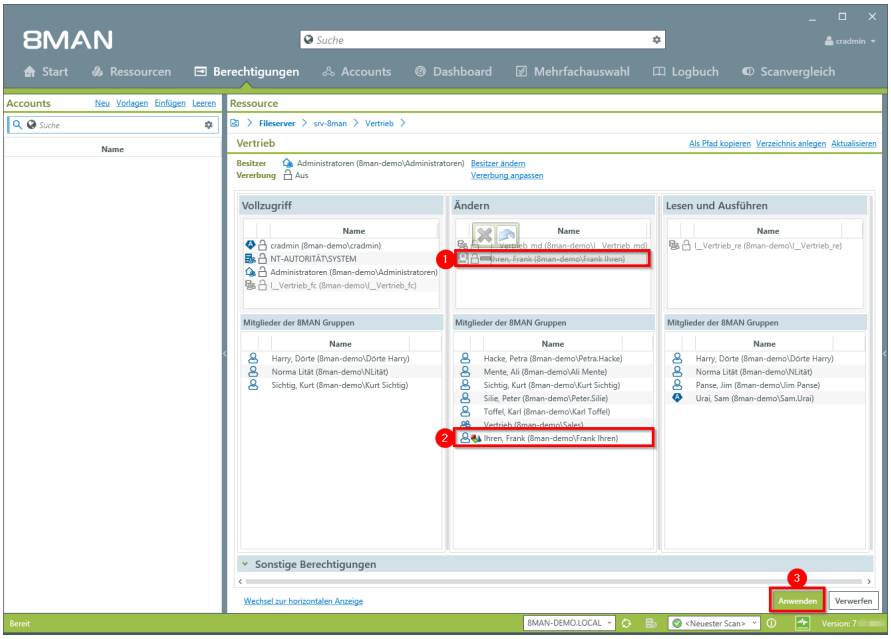
Der Prozess in einzelnen Schritten



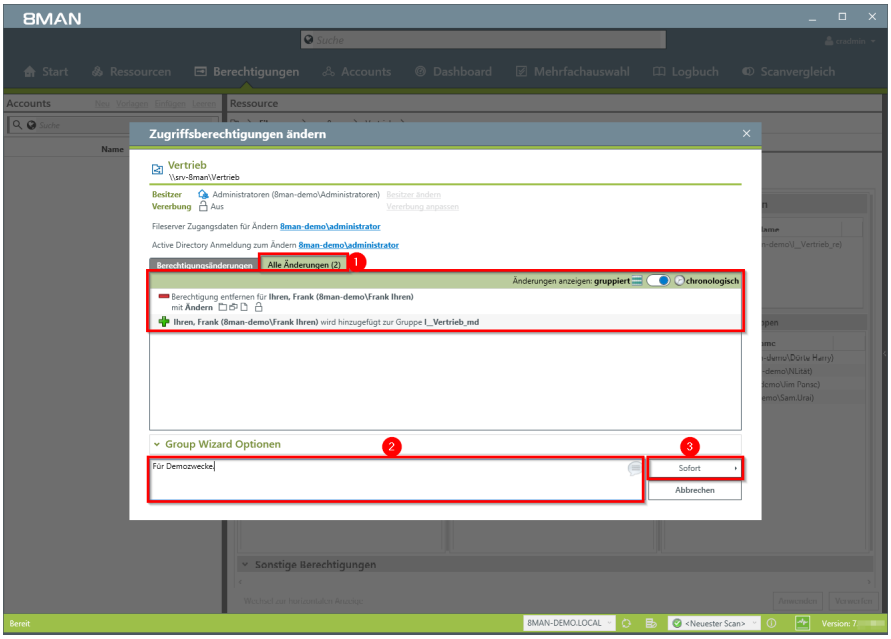
1. *Sie haben die Direktberechtigung identifiziert.*
2. *Rechtsklicken Sie auf das betreffende Verzeichnis.*
3. *Wählen Sie "Berechtigungen ändern..." im Kontextmenü.*



Ziehen Sie den Benutzer in die 8MAN-Gruppe.



1. *Die Direktberechtigung für "Frank Ihren" wird entfernt.*
2. *Die Gruppenmitgliedschaft wird erstellt.*
3. *Klicken Sie auf "Anwenden".*



1. *In der Detailansicht sehen Sie die Änderungsschritte.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie die Änderung.*

8.2.2.3 Broken ACLs identifizieren und mit Hilfe der Vererbung korrigieren

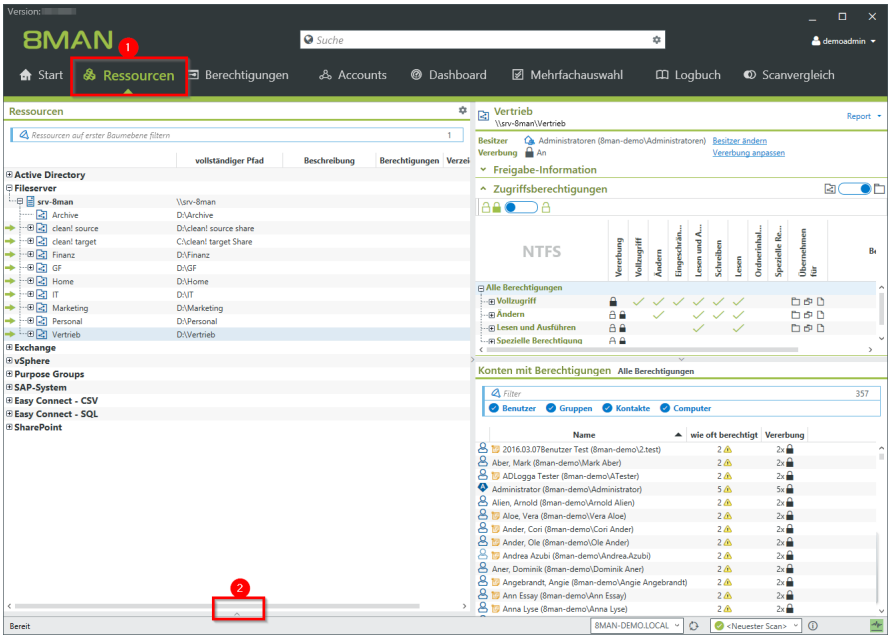
Hintergrund / Mehrwert

Sogenannte "Broken ACLs" (Access Control Lists) sind Fehler in der NTFS-Vererbung auf dem Fileserver. Die Folgen: Das Unterverzeichnis erhält nicht die korrekt vererbten Berechtigungen, obwohl die Vererbung aktiviert ist. 8MAN zeigt "Broken ACLs" und entfernt diese über die erneute Anwendung der Vererbungsfunktion.

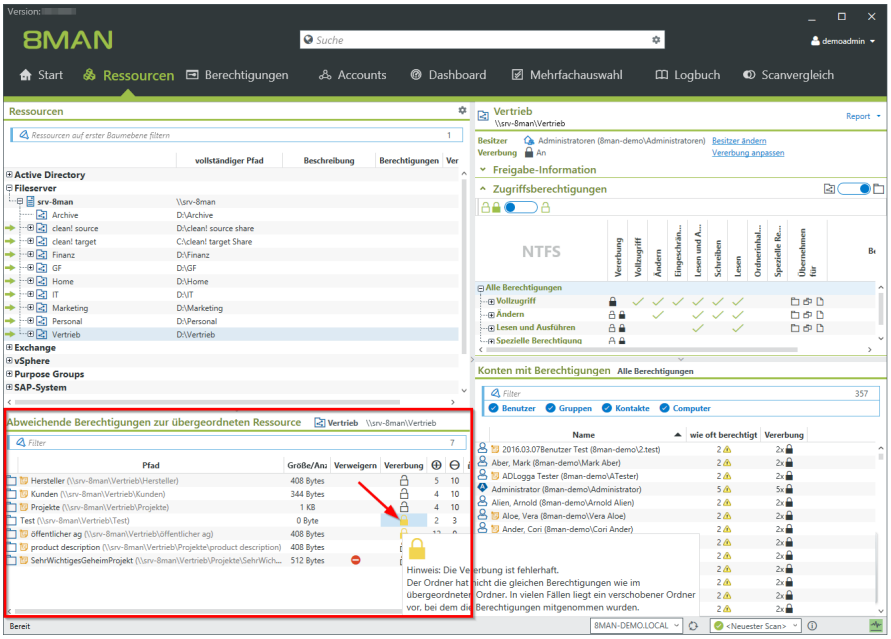
Weiterführende Services

Abweichende Berechtigungen im Bulk entfernen (Webclient)

Der Prozess in einzelnen Schritten



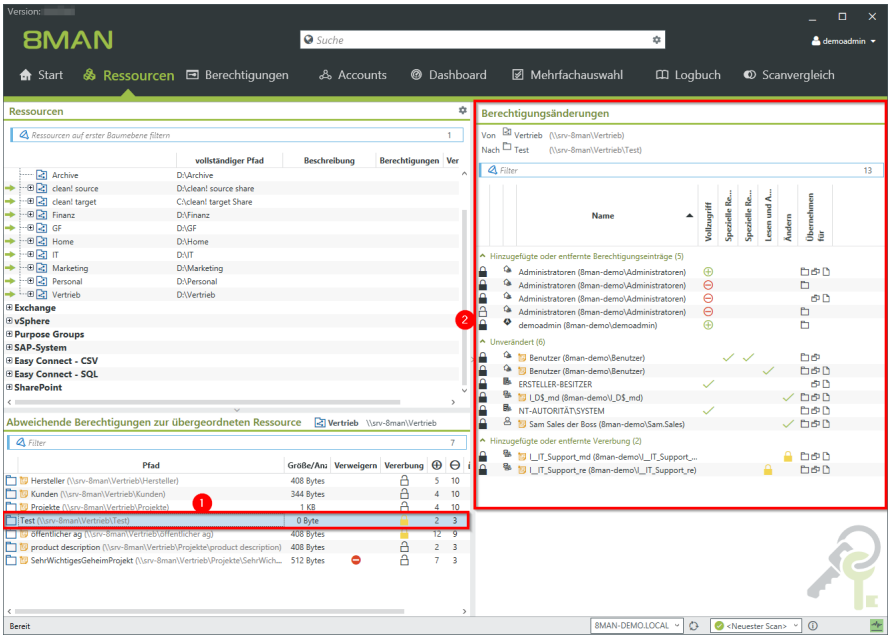
1. *Wählen Sie "Ressourcen".*
2. *Klappen Sie den Bereich auf.*



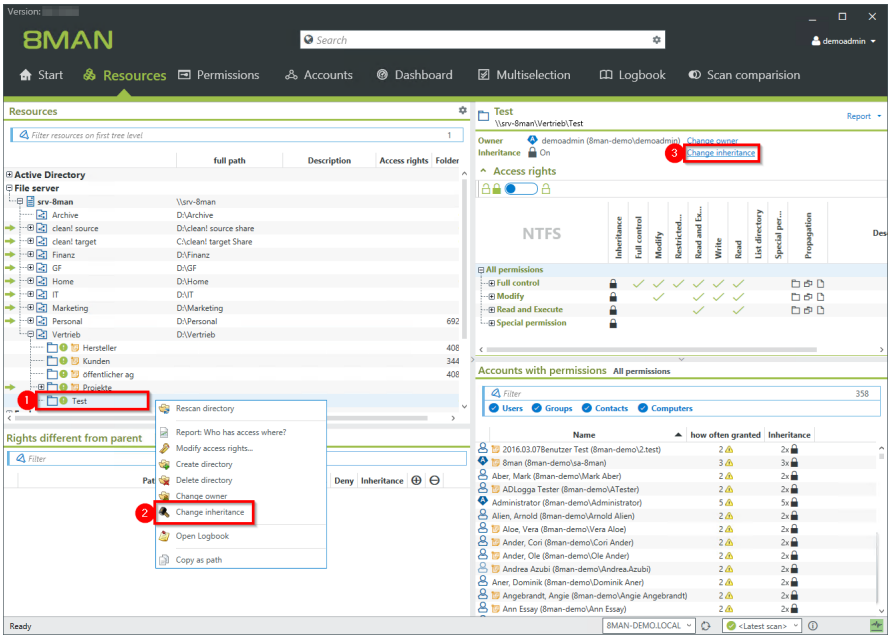
8MAN listet alle Unterverzeichnisse mit abweichenden Berechtigungen auf.

An dem gelben Schloss erkennen Sie eine fehlerhafte Vererbung.

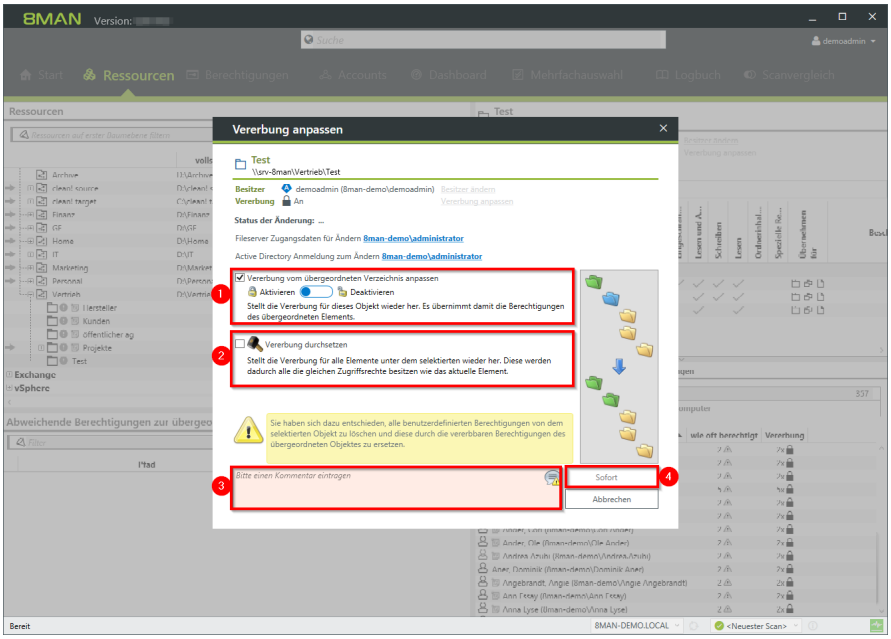
Nutzen Sie die Sortierfunktion in der Spalte "Vererbung".



1. *Klicken Sie auf einen Eintrag.*
2. *8MAN zeigt ihnen in allen Details, welche Berechtigungen sich im Vergleich zum übergeordneten Verzeichnis ändern.*



1. *Navigieren Sie zu dem Unterverzeichnis, bei dem Sie die fehlerhafte Vererbung korrigieren wollen.*
2. *oder 3. Klicken Sie auf "Vererbung anpassen".*



1. *Aktivieren Sie die Vererbung.*
2. *Setzen Sie die Vererbung auf die Unterverzeichnisse durch. Im Beispiel hier für alle Unterverzeichnisse von "Test".*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie die Ausführung.*

8.2.2.4 Verwaiste SIDs identifizieren und löschen

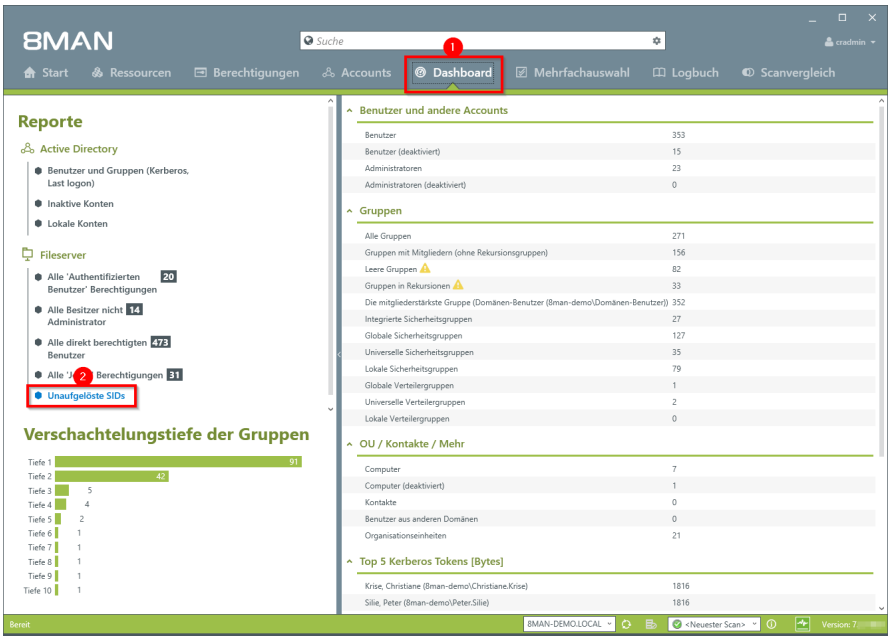
Hintergrund / Mehrwert

SIDs (Security Identifier) sind Zeichenfolgen, die einen Benutzer oder eine Gruppe eindeutig identifizieren. Werden Benutzer oder Gruppen gelöscht, bleiben verwaiste SIDs bestehen.
Mit Hilfe der verwaisten SID können Innentäter sich Zugriff auf Ressourcen verschaffen .
8MAN identifiziert verwaiste SIDs in Ihrem System. Diese können Sie im Anschluss löschen.

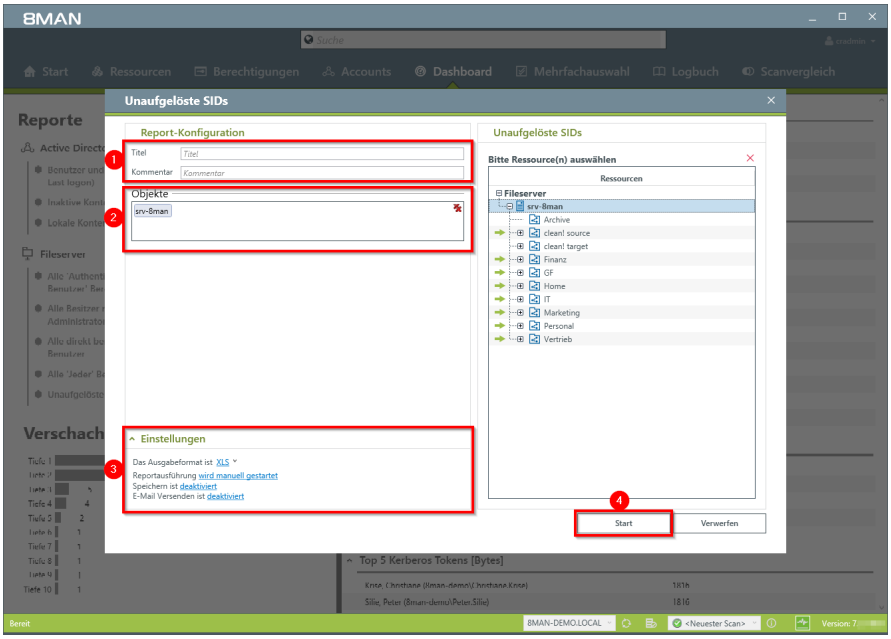
Weiterführende Services

Verwaiste SIDs im Bulk löschen (Webclient)

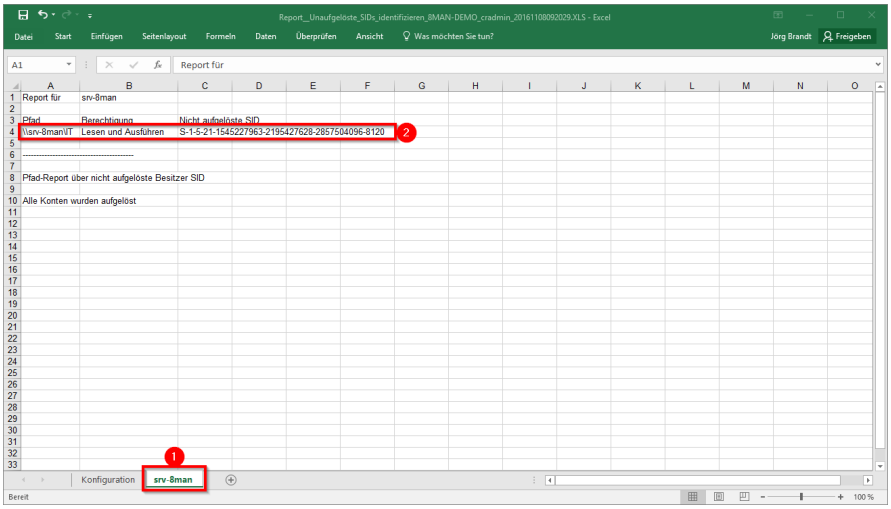
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Dashboard".*
2. *Klicken Sie auf "Unaufgelöste SIDs".*

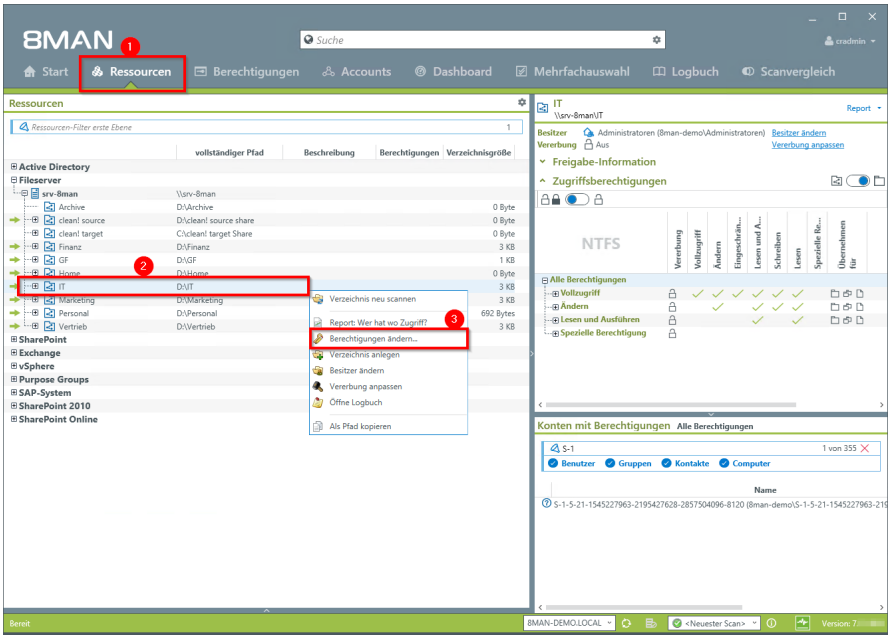


1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Definieren Sie den Umfang des Reports.*
3. *Legen Sie verschiedene Ausgabeoptionen fest.*
4. *Starten Sie die Erstellung des Reports.*

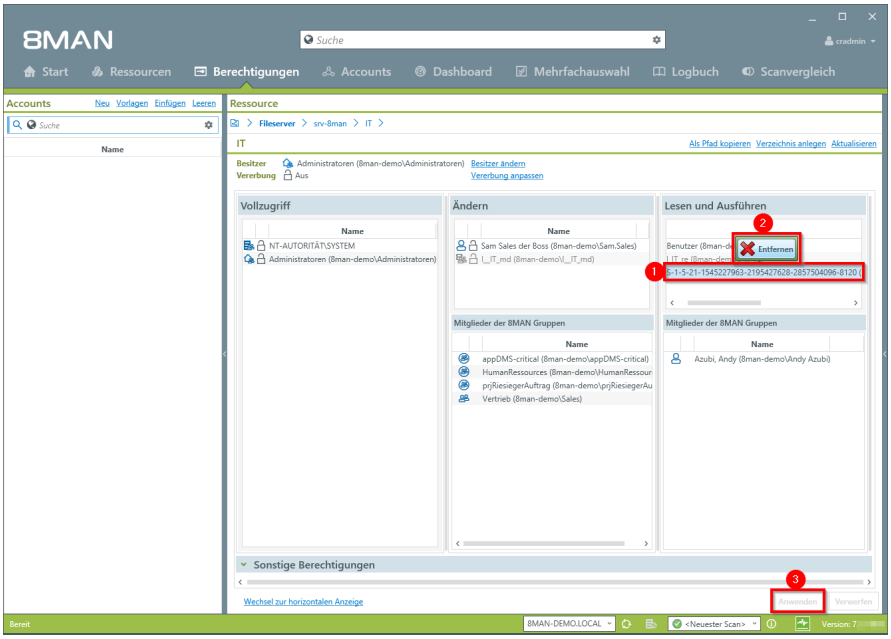


Öffnen Sie den Report in Excel.

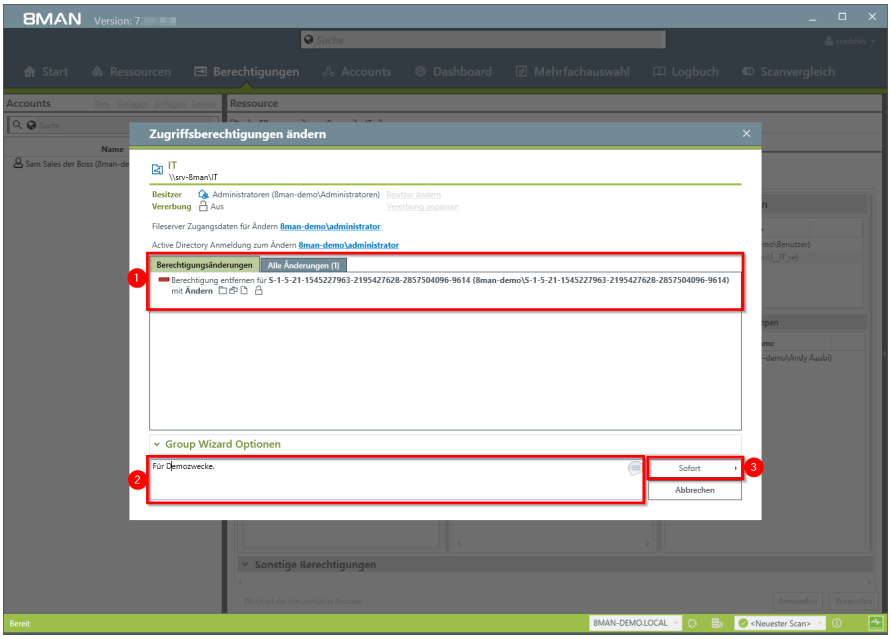
1. *Wechseln Sie in das Fileserver-Tabellenblatt.*
2. *In dem Report sind alle nicht aufgelösten SIDs aufgelistet.*



1. *Wählen Sie "Ressourcen".*
2. *Selektieren Sie ein betroffenes Verzeichnis.*
3. *Rechtsklicken Sie auf das Verzeichnis und klicken Sie auf "Berechtigungen ändern..." im Kontextmenü.*



1. *Selektieren Sie die SID.*
2. *Klicken Sie auf "Entfernen".*
3. *Klicken Sie auf "Anwenden".*



1. *8MAN listet die geplanten Änderungen auf.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie das Entfernen.*

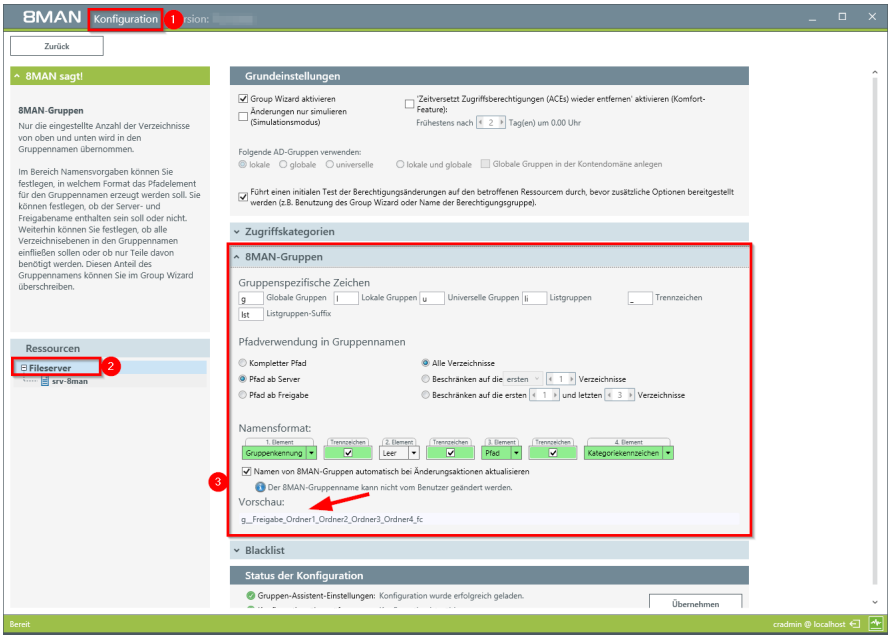
8.2.2.5 Namenskonventionen für Berechtigungsgruppen festlegen

Hintergrund / Mehrwert

8MAN beendet nicht standardisierte Gruppenbezeichnungen. Administratoren einigen sich auf ein Namensschema und die Einhaltung wird bei der Neuerstellung von Berechtigungsgruppen durch 8MAN sichergestellt.

Die Einstellungen nehmen Sie in der 8MAN Konfigurationsoberfläche vor.

Der Prozess in einzelnen Schritten



1. *Navigieren Sie in der 8MAN Konfigurationsoberfläche zu "Ändern-Konfiguration" -> "Fileserver".*
2. *Selektieren Sie die gewünschte Fileserver-Ressource.*
3. *Legen Sie die Namenskonventionen fest. Beachten Sie, dass 8MAN Ihnen eine Vorschau anzeigt.*

8.2.2.6 Den Besitzer von Verzeichnissen ändern

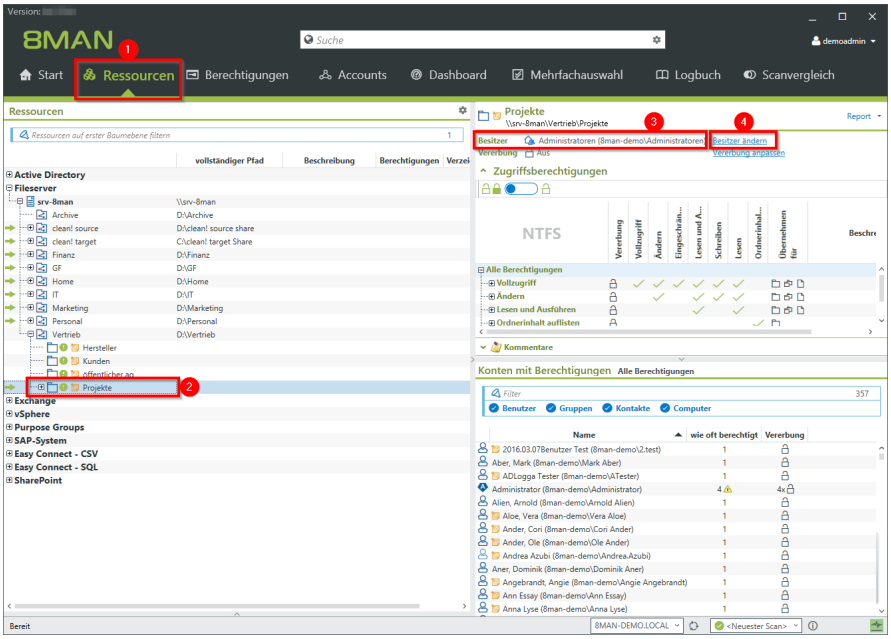
Hintergrund / Mehrwert

Mit 8MAN ändern Sie einfach den Besitzer von Verzeichnissen. Schließen Sie die User vom Besitz von Verzeichnissen aus, können Sie unerwünschte Berechtigungsänderungen verhindern.

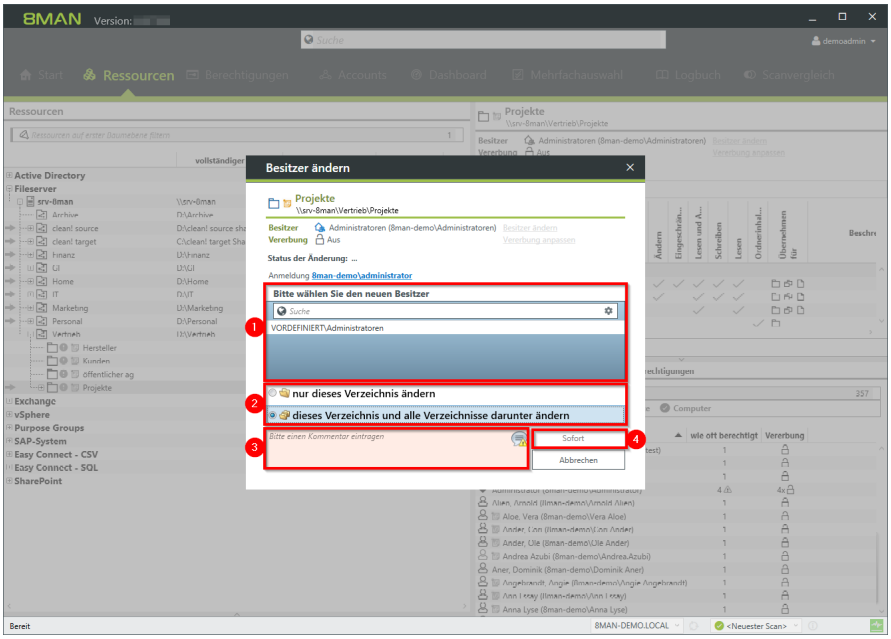
Weiterführende Services

Verzeichnisse identifizieren, deren Besitzer nicht Administratoren sind (Report)

Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Navigieren Sie zum gewünschten Verzeichnis. Alternativ nutzen Sie die Suche.*
3. *8MAN zeigt Ihnen den aktuellen Besitzer.*
4. *Klicken Sie auf "Besitzer ändern".*



1. *Wählen Sie einen neuen Besitzer.*
2. *Legen Sie fest, ob die Änderung nur für das aktuelle oder auch für alle untergeordneten Verzeichnisse durchgeführt wird.*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie die Ausführung.*

8.2.2.7 Fehler in der Vererbung in Analyze&Act identifizieren und im Bulk beheben

Hintergrund / Mehrwert

Fehler in der Vererbung von Fileserverberechtigungen treten häufig auf, wenn Mitarbeiter Verzeichnisse kopieren oder verschieben. Dies kann zu unerwünschten Zugriffen führen.

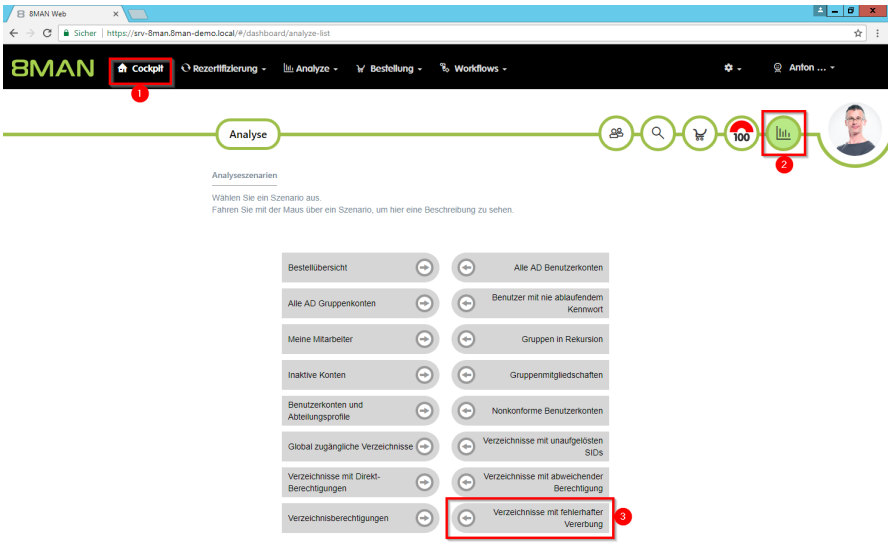
Mit dem Szenario "Verzeichnisse mit fehlerhafter Vererbung" identifizieren Sie mit wenigen Klicks die Vererbungsfehler und beseitigen diese in einem Rutsch durch Wiederherstellen der Vererbung.

Weiterführende Services

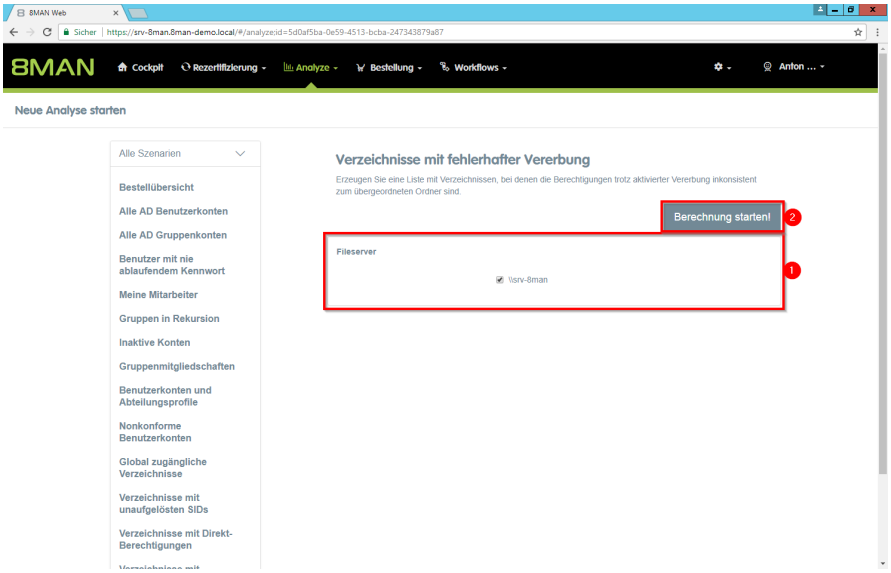
Wiederkehrende Änderungsaufgaben planen

Broken ACLs identifizieren und mit Hilfe der Vererbung korrigieren (Rich Client)

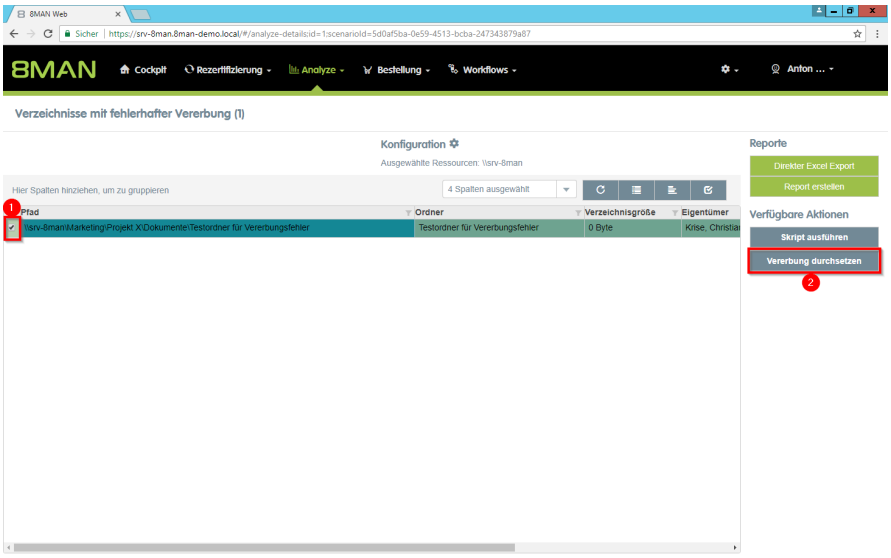
Der Prozess in einzelnen Schritten



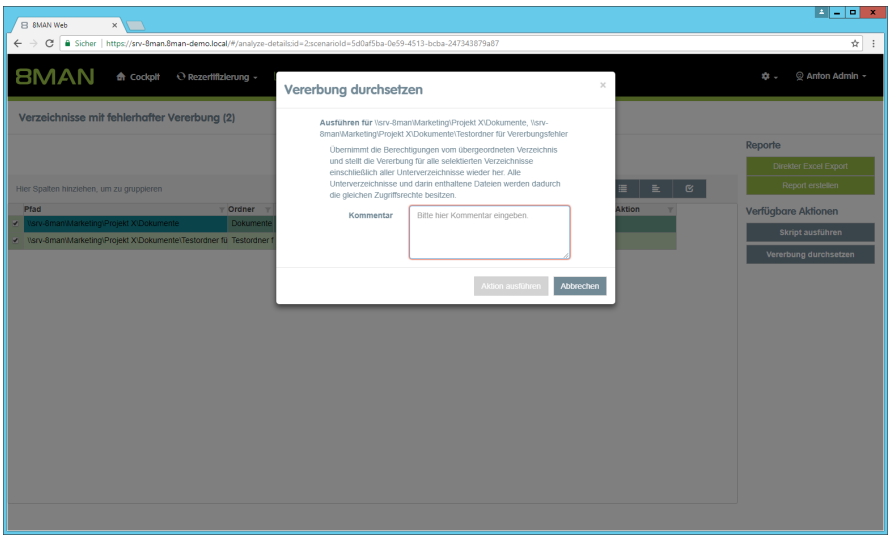
Wählen Sie im Cockpit "Analyse" und dann "Verzeichnisse mit fehlerhafter Vererbung".



1. *Legen Sie fest, welche Fileserver in Ihrer Analyse enthalten sind.*
2. *Starten Sie die Berechnung.*



1. *Selektieren Sie die Verzeichnisse, bei denen Sie die Vererbungsfehler korrigieren wollen.*
2. *Klicken Sie auf Vererbung durchsetzen.*



Sie sehen, für welche Verzeichnisse die Vererbung wieder durchgesetzt wird.

Sie müssen einen Kommentar eingeben.

8.3 +8MATE for Exchange

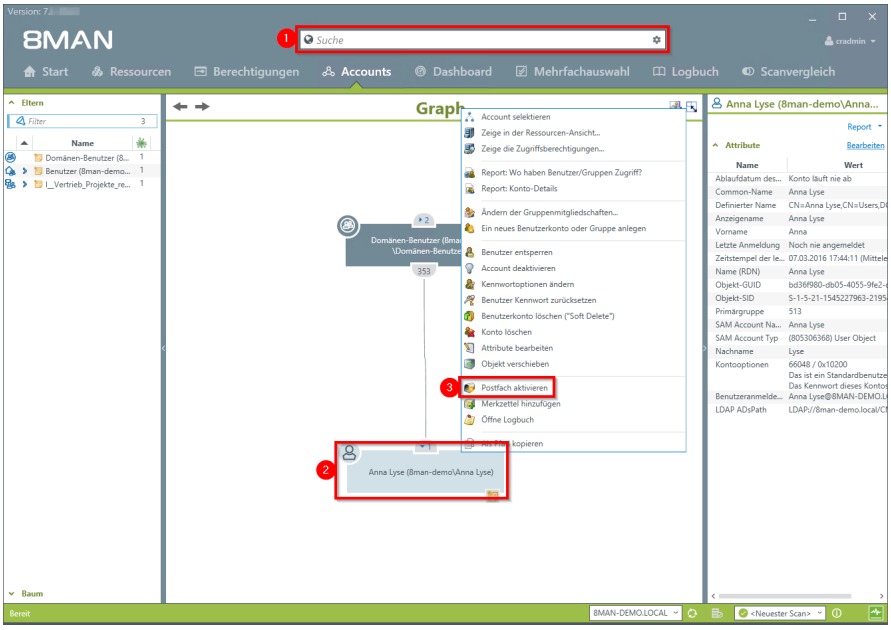
8.3.1 Help Desk

8.3.1.1 Ein Postfach anlegen

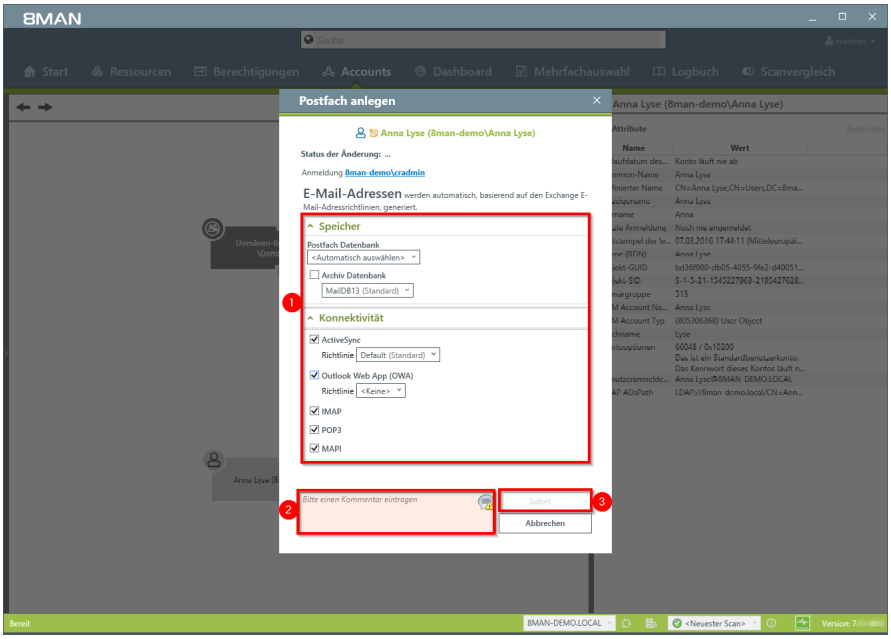
Hintergrund / Mehrwert

Verfügen Sie über den 8MATE for Exchange, können Sie Postfächer über 8MAN aktivieren.

Der Prozess in einzelnen Schritten



1. *Suchen Sie den gewünschten Benutzer oder eine Verteilergruppe vom Typ Universell.*
2. *Rechtsklicken Sie den Account, z. B. in der Accounts-Ansicht.*
3. *Klicken Sie im Kontextmenü auf "Postfach aktivieren". Die Option ist nur sichtbar, wenn noch kein Postfach vorhanden ist.*



1. *Legen Sie Exchange Optionen fest.*
2. *Sie müssen einen Kommentar eingeben, z. B. eine Ticketnummer..*
3. *Starten Sie das Erstellen des Postfachs.*

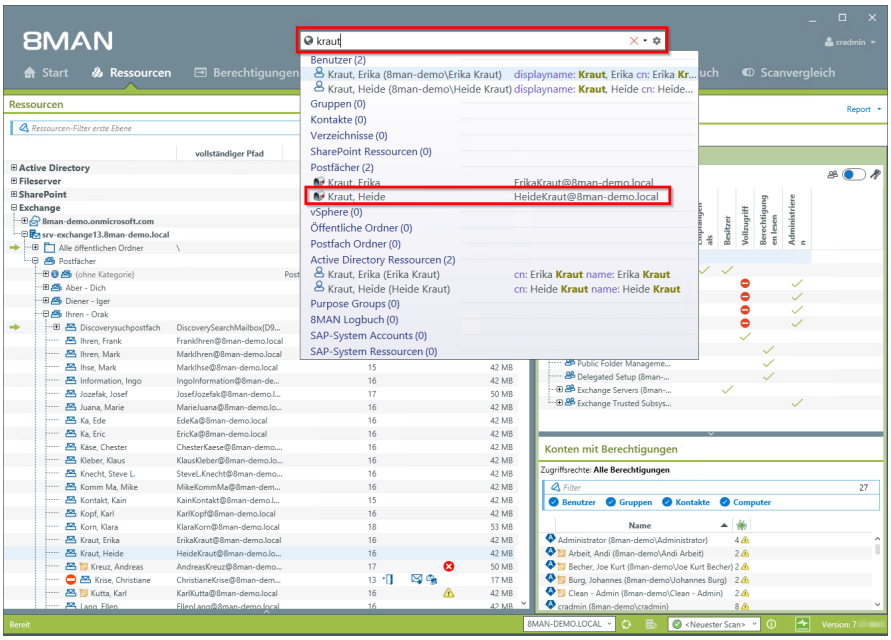
8.3.1.2 Berechtigungen auf Postfächer ändern

Hintergrund / Mehrwert

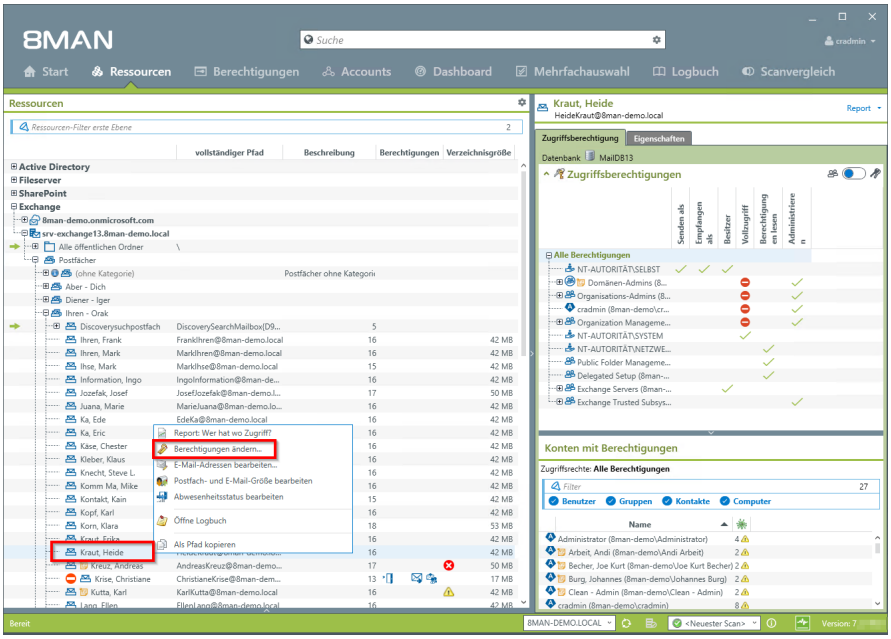
Der 8MATE Exchange zeigt die Zugriffsrechte auf Postfächer in der Ressource-Ansicht. Unterschieden wird zwischen "Besitzer", "Vollzugriff" , "Berechtigungen lesen" und "Administrieren".

Darüber hinaus können Sie einzelnen Nutzern "Vollzugriff", "Senden als", "Senden im Auftrag von" und "Empfangen als" Berechtigungen vergeben.

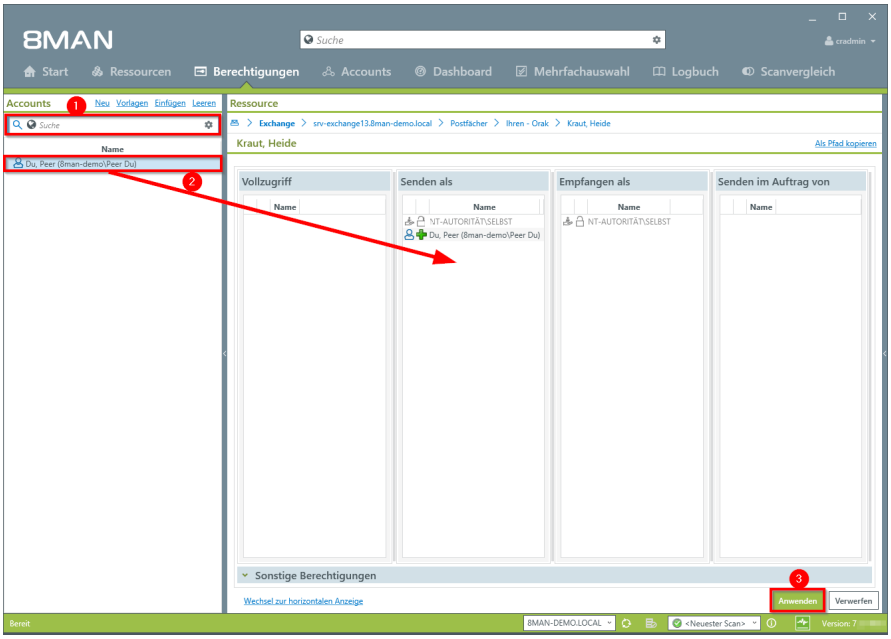
Der Prozess in einzelnen Schritten



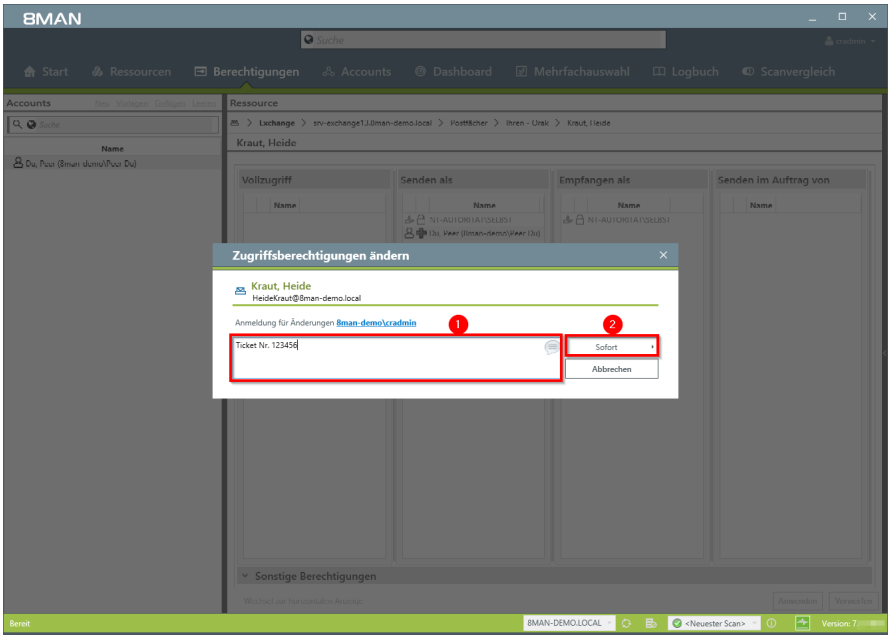
Nutzen Sie die Suche, um das gewünschte Postfach zu finden.



Klicken Sie mit der rechten Maustaste auf das Postfach und wählen "Berechtigungen ändern..." im Kontextmenü.



1. *Nutzen Sie die Suche, um den gewünschten Account zu finden. In den Suchoptionen (Zahnrad) muss die Option "Exchange Account" aktiviert sein.*
2. *Ziehen Sie den Account per Drag&Drop auf eine Berechtigungsspalte.*
3. *Klicken Sie auf "Anwenden".*



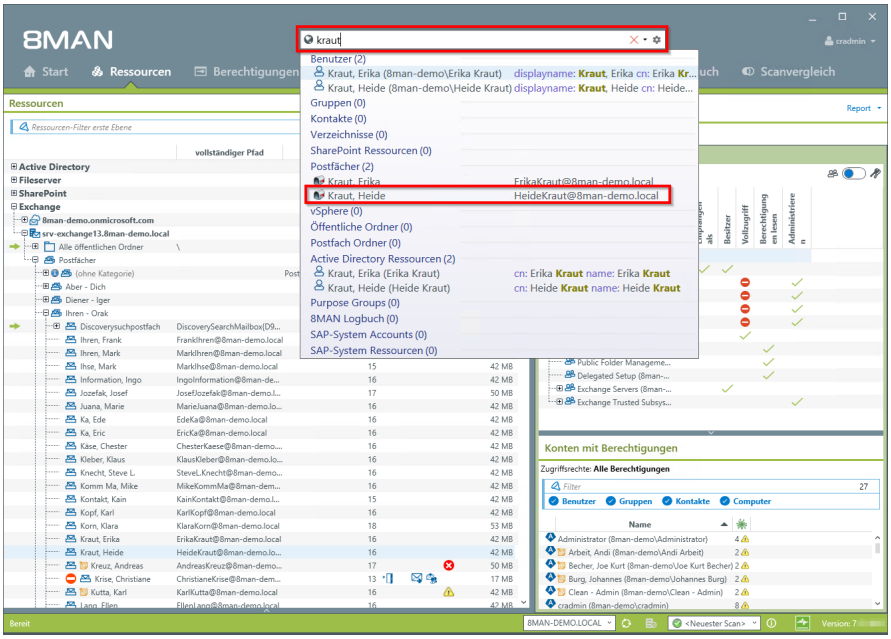
1. *Sie müssen einen Kommentar eingeben, z. B. eine Ticketnummer.*
2. *Starten Sie die Berechtigungsänderung.*

8.3.1.3 Abwesenheitsnotizen ändern

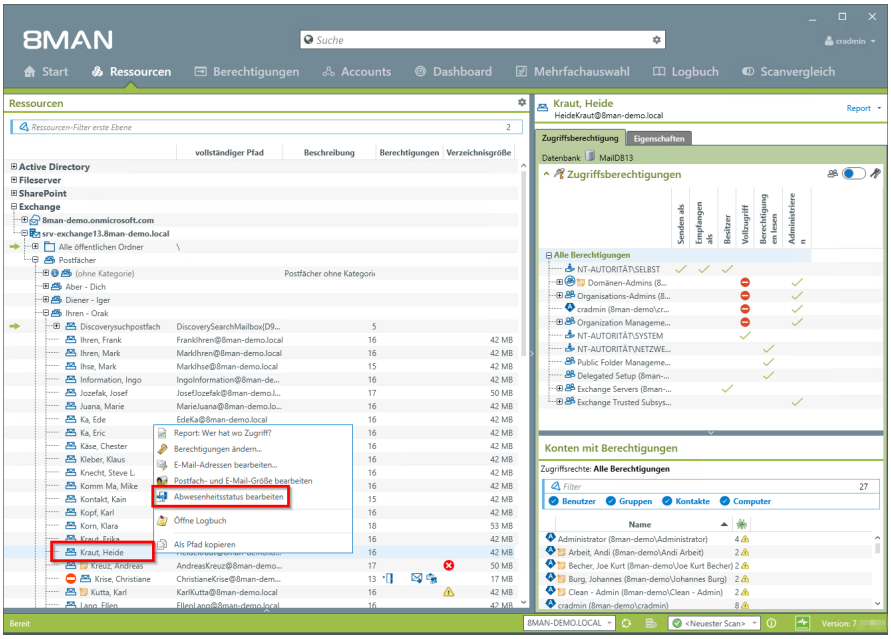
Hintergrund / Mehrwert

Mit 8MAN kann der Helpdesk Abwesenheitsnotizen für Mitarbeiter einstellen. Der Zugriff auf Postfachinhalte bleibt dem Servicedesk Mitarbeiter verwehrt.

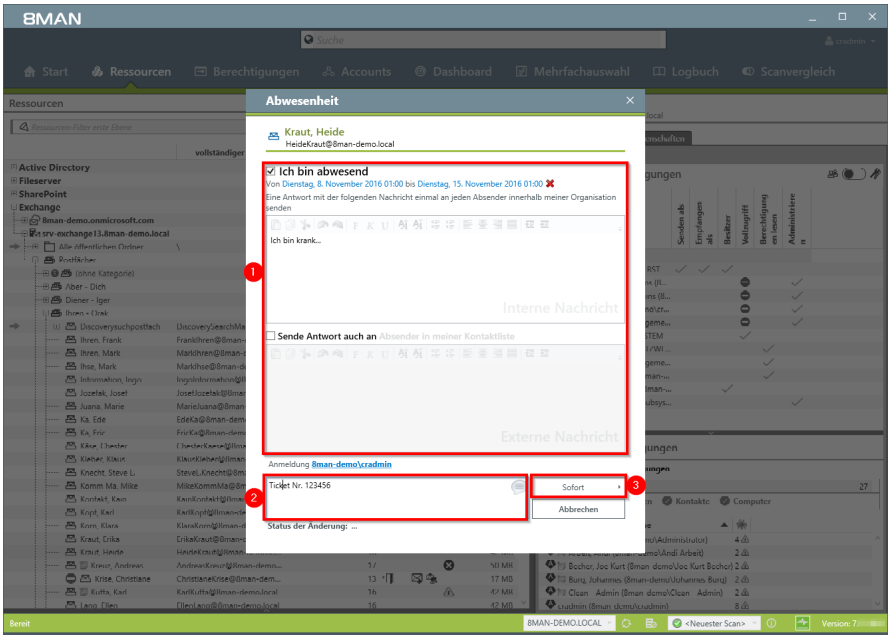
Der Prozess in einzelnen Schritten



Benutzen Sie die Suche, um das gewünschte Postfach zu finden.



Klicken Sie mit der rechten Maustaste auf das Postfach und wählen "Abwesenheitsstatus bearbeiten" im Kontextmenü.



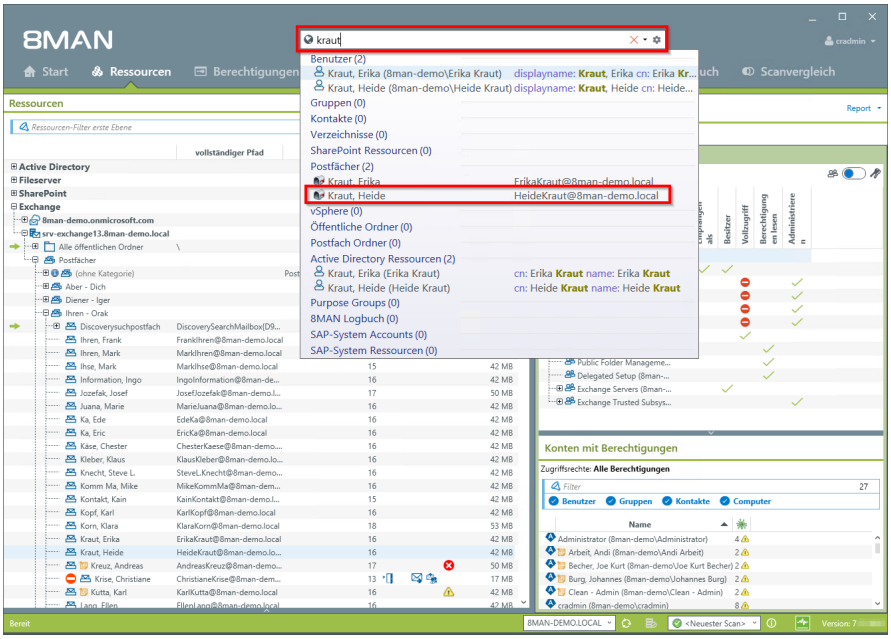
1. *Legen Sie die Abwesenheitseinstellungen fest.*
2. *Sie müssen einen Kommentar eingeben, z. B. eine Ticketnummer.*
3. *Starten Sie die Ausführung.*

8.3.1.4 Postfach- und E-Mail-Größen ändern

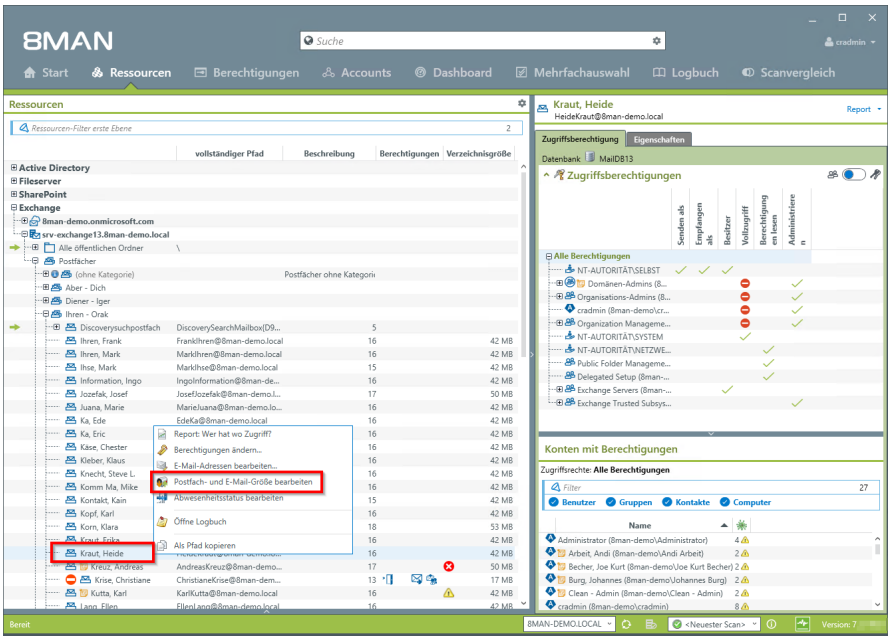
Hintergrund / Mehrwert

Ein häufig auftretender Task für den Helpdesk ist die Anpassung der Postfachgröße. Deshalb erlaubt 8MAN die Anpassungen schnell vorzunehmen.

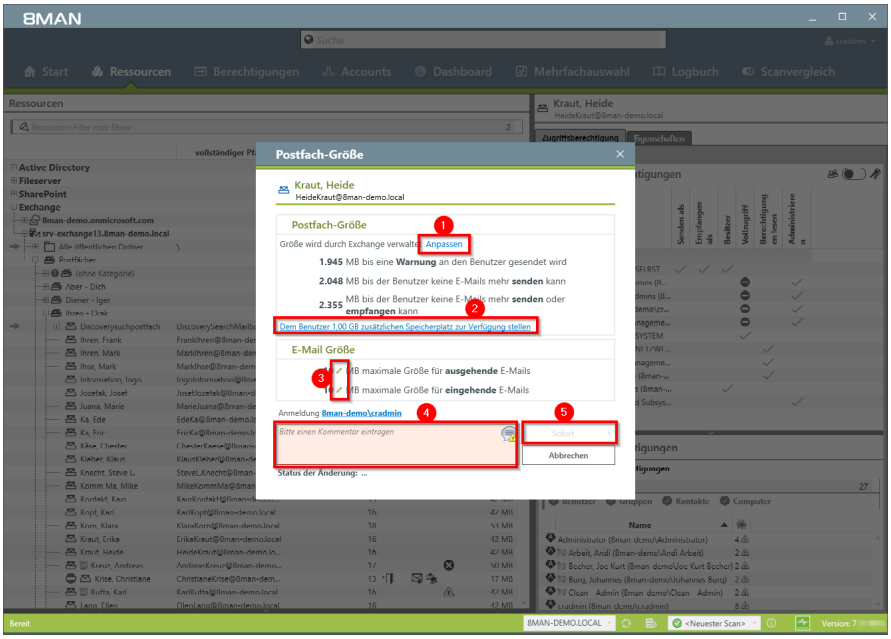
Der Prozess in einzelnen Schritten



Benutzen Sie die Suche, um das gewünschte Postfach zu finden.



Klicken Sie mit der rechten Maustaste auf das Postfach und wählen "Postfach- und E-Mail-Größe bearbeiten" im Kontextmenü.



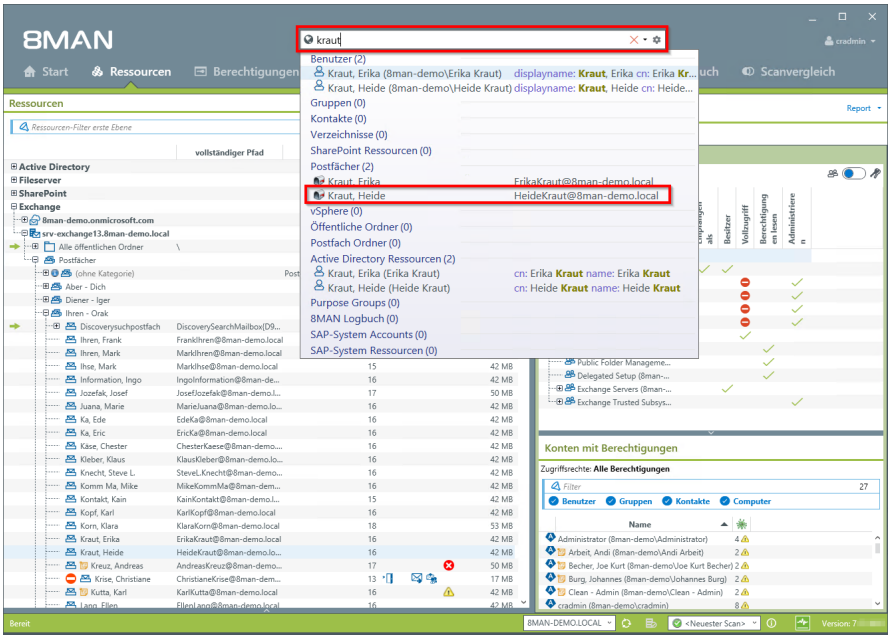
1. *Klicken Sie auf "Anpassen", um die Postfachgrößen genau einzustellen.*
2. *Stellen Sie schnell 1 GB zusätzlichen Speicherplatz zur Verfügung. Die Schrittweite kann in der Konfiguration angepasst werden.*
3. *Klicken Sie auf das Stift-Symbol, um die maximalen E-Mail-Größen einzustellen.*
4. *Sie müssen einen Kommentar eingeben, z. B. die Ticketnummer.*
5. *Starten Sie die Ausführung.*

8.3.1.5 E-Mail-Adressen bearbeiten

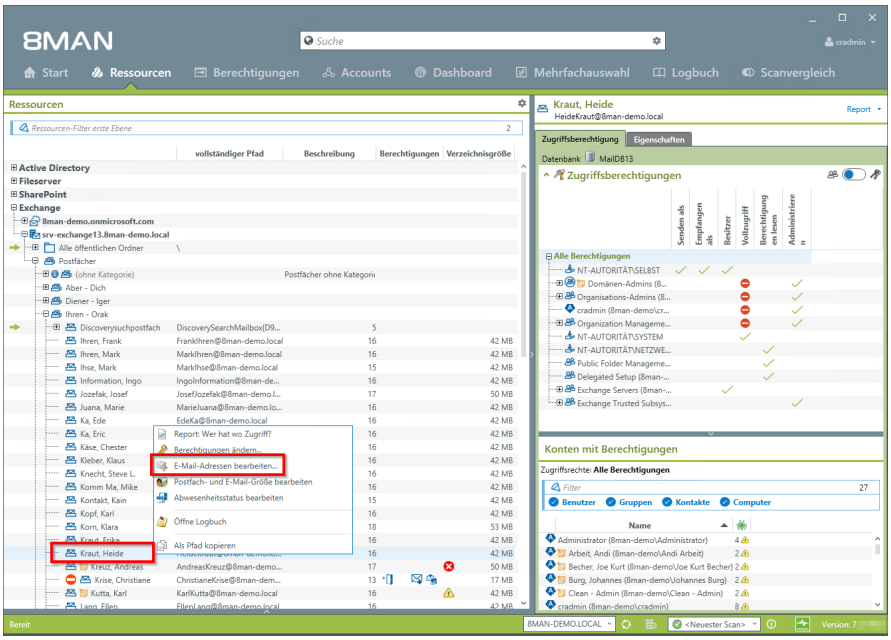
Hintergrund / Mehrwert

Mit 8MAN können Sie Postfächern, Verteilergruppen und Kontakten weitere E-Mail-Adressen zuordnen bzw. bestehende löschen oder ändern. Der Prozess wird automatisch dokumentiert.

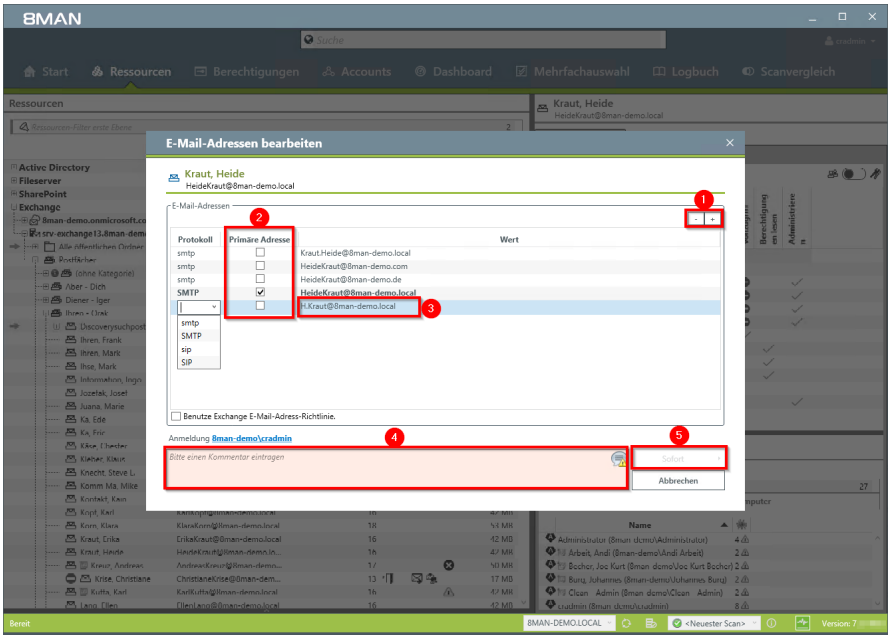
Der Prozess in einzelnen Schritten



Benutzen Sie die Suche, um das gewünschte Postfach zu finden.



Klicken Sie mit der rechten Maustaste auf das Postfach und wählen "E-Mail-Adressen bearbeiten..." im Kontextmenü.



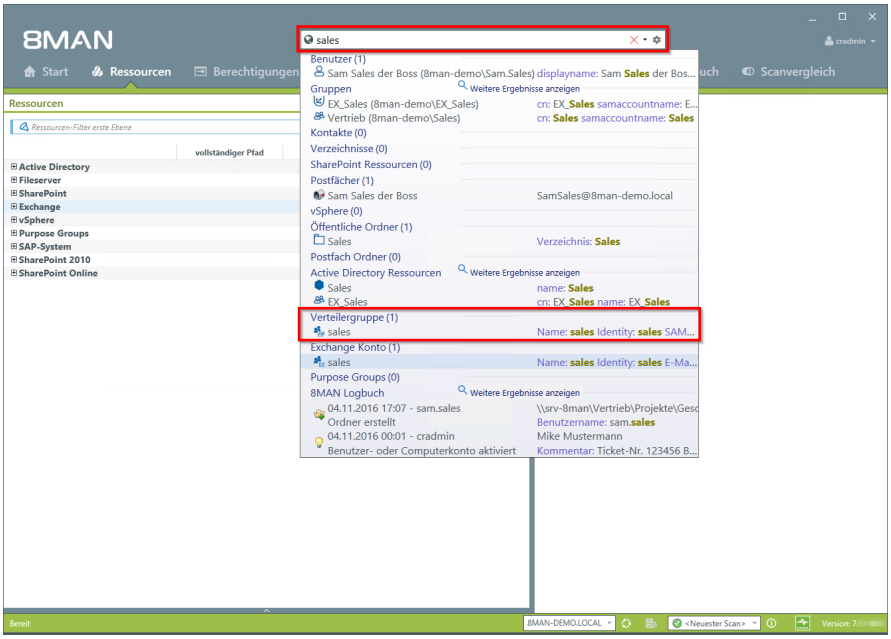
1. *Fügen Sie eine E-Mail-Adresse hinzu oder löschen Sie eine bereits vorhandene.*
2. *Wählen Sie die primäre E-Mail-Adresse.*
3. *Doppelklicken Sie in das Feld, um eine Adresse zu ändern oder einzugeben.*
4. *Sie müssen einen Kommentar eingeben, z. B. die Ticketnummer.*
5. *Starten Sie die Ausführung der E-Mail-Adressänderung.*

8.3.1.6 Mitgliedschaften von Verteilergruppen bearbeiten

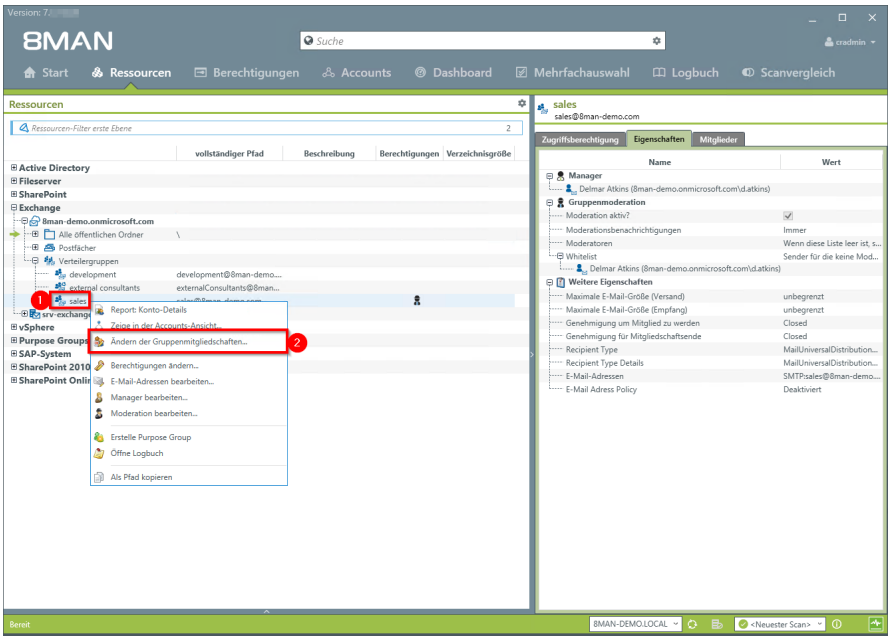
Hintergrund / Mehrwert

Mit 8MAN bearbeiten Sie einfach die Mitgliedschaften von Verteilergruppen. Dazu gehört das Hinzufügen oder Entfernen von Empfängern als auch die Verschachtelung mit anderen Gruppen (Eltern-Kind-Beziehungen). Der Prozess wird automatisch dokumentiert.

Der Prozess in einzelnen Schritten

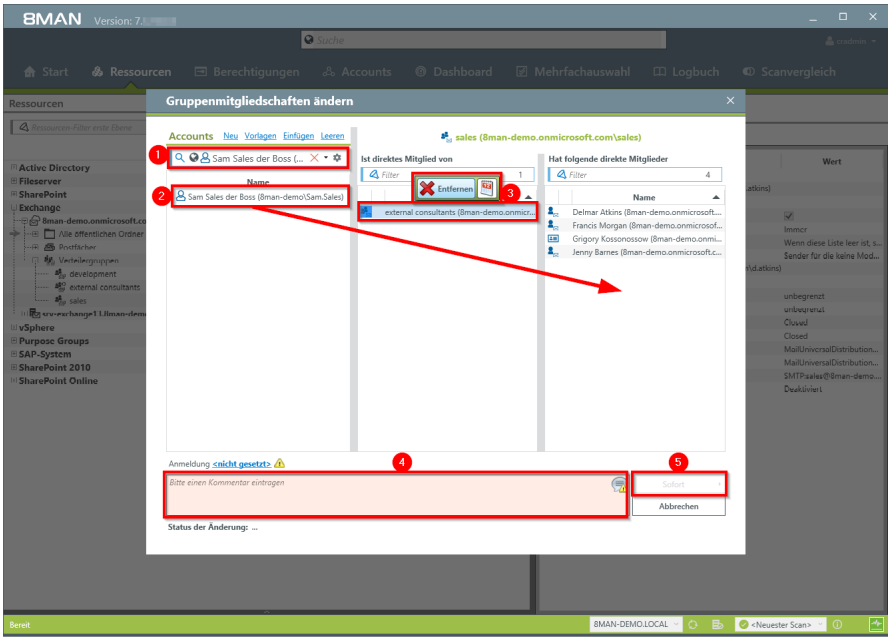


Nutzen Sie die Suche, um die gewünschte Verteilergruppe zu finden.



1. *Sie haben die gewünschte Gruppe im Fokus.*
2. *Rechtsklicken Sie auf die Gruppe und wählen "Ändern der Gruppenmitgliedschaften..."*

.



1. *Nutzen Sie die Suche, um einen Account zu finden. In den Suchoptionen (Zahnrad) muss die Option "Exchange Account" aktiviert sein.*
2. *Ziehen Sie den Account per Drag&Drop auf eine Spalte, um eine Mitgliedschaft zuzuweisen.*
3. *Mit der "Entfernen" Schaltfläche können Sie Mitgliedschaften beenden.*
4. *Sie müssen einen Kommentar eingeben, z. B. eine Ticketnummer.*
5. *Starten Sie die Änderung.*

8.3.1.7 Berechtigungen auf Verteilergruppen bearbeiten

Hintergrund / Mehrwert

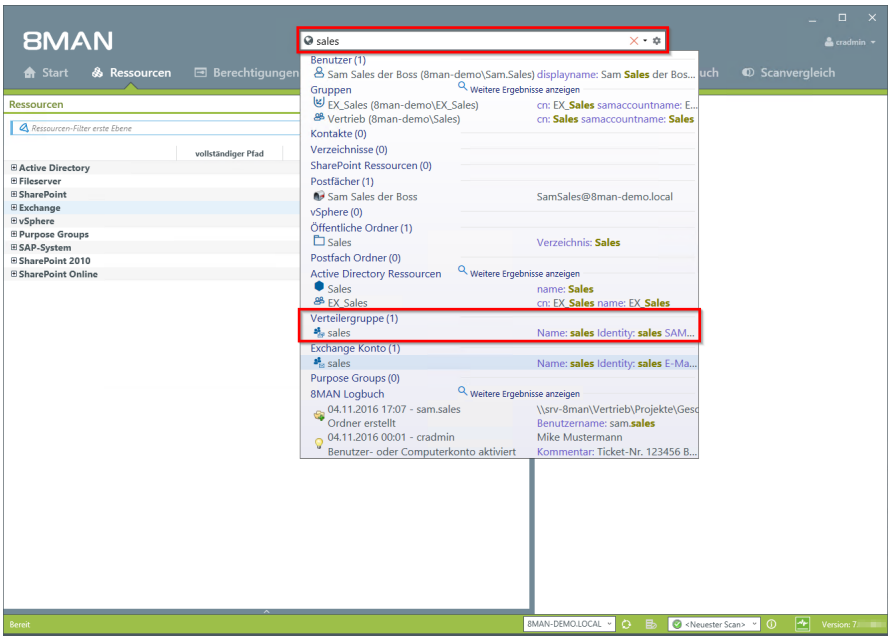
Mit 8MAN ändern Sie schnell, wer über welchen Verteiler E-Mails verschicken kann. Der Prozess wird automatisch dokumentiert.

Relevant sind die beiden Fälle „Senden als“ und „Senden im Auftrag von“:

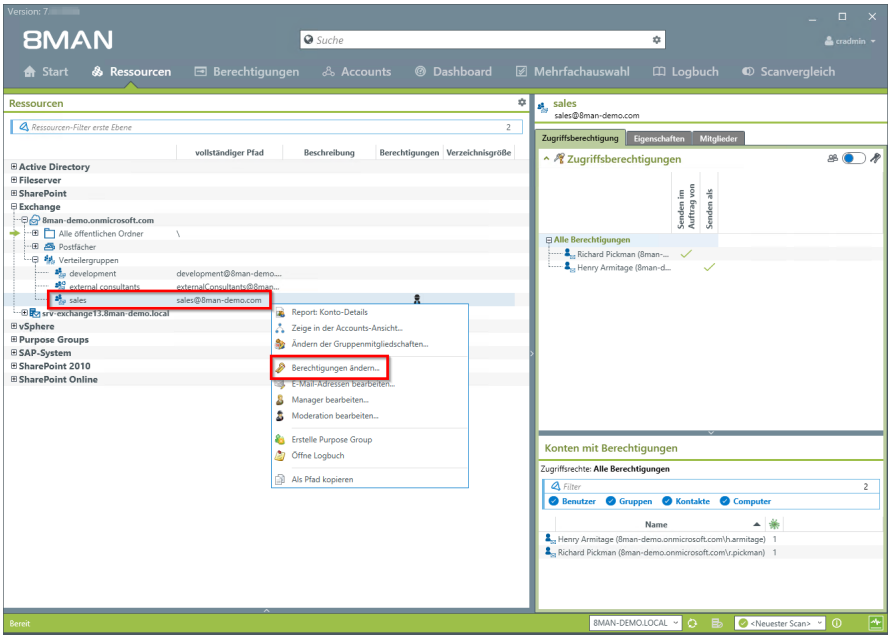
Der Erstgenannte ist besonders brisant, weil nicht ersichtlich ist, wer tatsächlich die Mail verschickt hat.

Bei „Senden im Auftrag von“ ist z. B. der Sekretär / die Sekretärin, die im Auftrag versendet, für den Empfänger erkennbar.

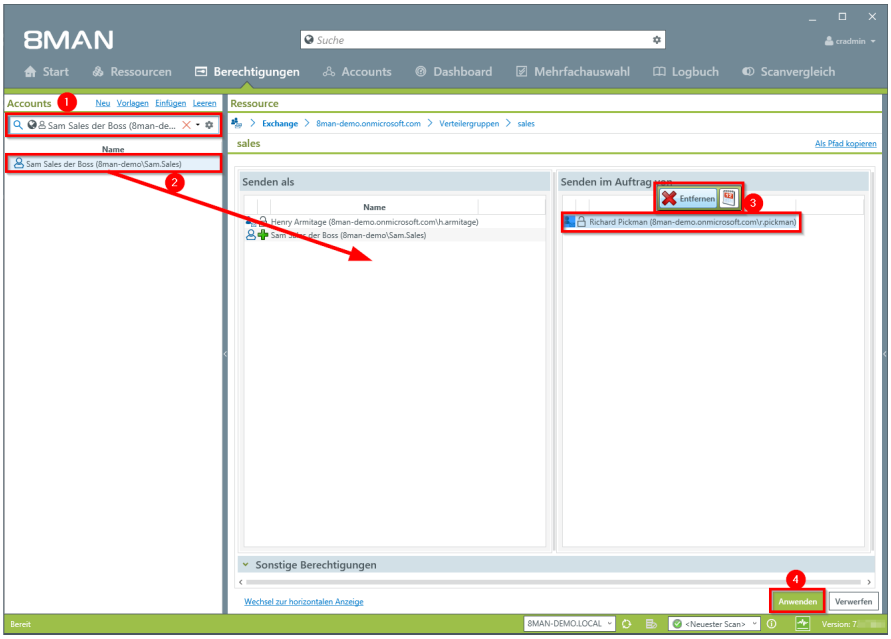
Der Prozess in einzelnen Schritten



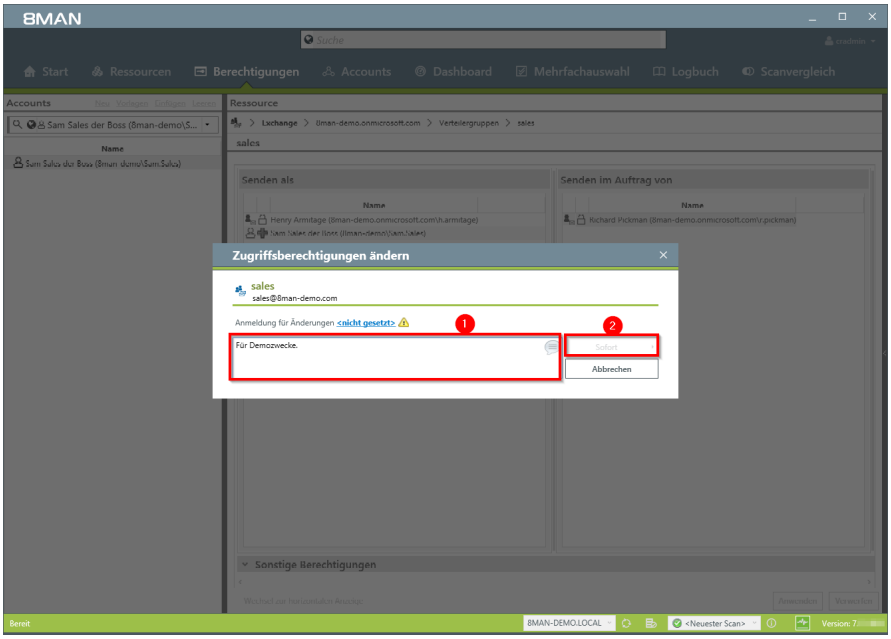
Nutzen Sie die Suche, um die gewünschte Verteilergruppe zu finden.



Rechtsklicken Sie auf die gewünschte Verteilergruppe und wählen "Berechtigungen ändern..." im Kontextmenü.



1. *Nutzen Sie die Suche, um einen Account zu finden. In den Suchoptionen (Zahnrad) muss die Option "Exchange Account" aktiviert sein.*
2. *Ziehen Sie den Account auf eine Zugriffspalte, um eine Berechtigung zuzuweisen.*
3. *Selektieren Sie einen Eintrag und klicken auf "Entfernen" im Kontextmenü, um eine Berechtigung zu entziehen.*
4. *Klicken Sie auf "Anwenden".*



1. *Sie müssen einen Kommentar eingeben.*
2. *Starten Sie die Berechtigungsänderung.*

8.3.1.8 Moderation von Verteilergruppen ändern

Hintergrund / Mehrwert

Mit 8MAN können Sie schnell die Moderation von Verteilergruppen ändern. Der Prozesse wird automatisch dokumentiert.

Sind keine Moderatoren mit spezifischen Freigaberechten nominiert, ist der Manager einziger Moderator.

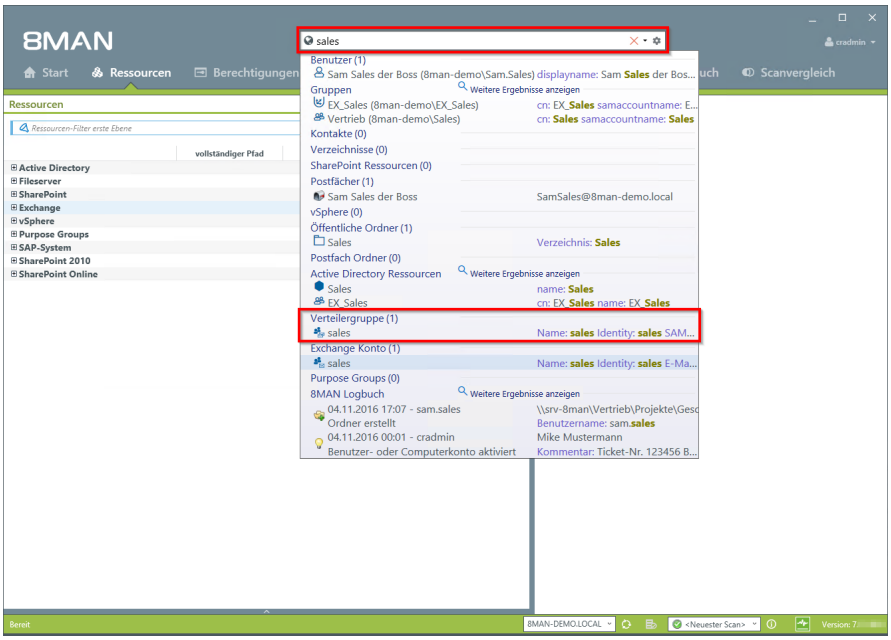
Weiterführende Services

Eigenschaften von Verteilergruppen anzeigen

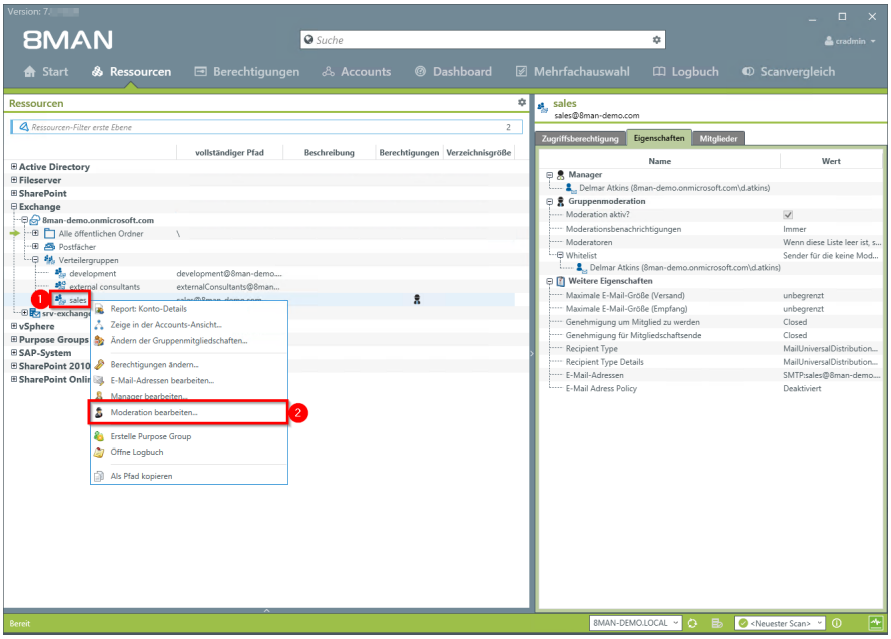
Manager von Verteilergruppen ändern

Die Änderung funktioniert auch bei dynamischen Exchange-Gruppen.

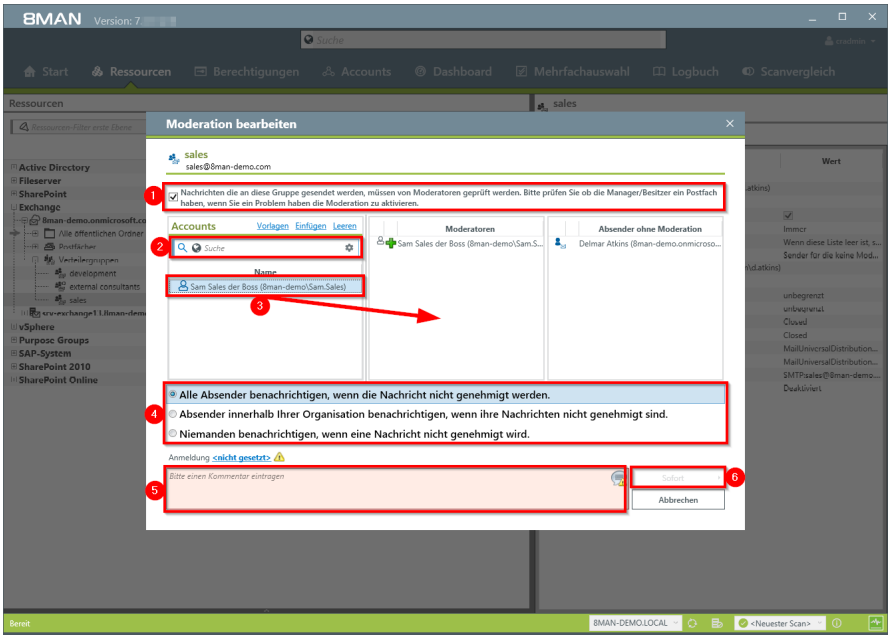
Der Prozess in einzelnen Schritten



Nutzen Sie die Suche, um die gewünschte Verteilergruppe zu finden.



1. *Sie haben die gewünschte Gruppe im Fokus.*
2. *Rechtsklicken Sie auf die Gruppe und wählen "Moderation bearbeiten...".*



1. *Aktivieren oder Deaktivieren Sie die Moderation der Verteilergruppe.*
2. *Nutzen Sie die Suche, um Accounts zu finden. In den Suchoptionen (Zahnrad) muss die Option "Exchange Account" aktiviert sein.*
3. *Mit Drag&Drop können Sie Accounts auf die Spalte "Moderatoren" oder "Absender ohne Moderation" (Whitelist) ziehen.*
4. *Legen Sie fest, wie mit abgelehnten Nachrichten verfahren wird.*
5. *Sie müssen einen Kommentar eingeben, z. B. eine Ticketnummer.*
6. *Starten Sie die Ausführung.*

8.3.1.9 Manager von Verteilergruppen ändern

Hintergrund / Mehrwert

Mit 8MAN können Sie schnell die Manager von Verteilergruppen ändern. Der Prozess wird automatisch dokumentiert.

Manager sind im Standard die einzigen, die Verteilerguppen außerhalb von 8MAN konfigurieren dürfen, z. B. im Exchange Admin Center.

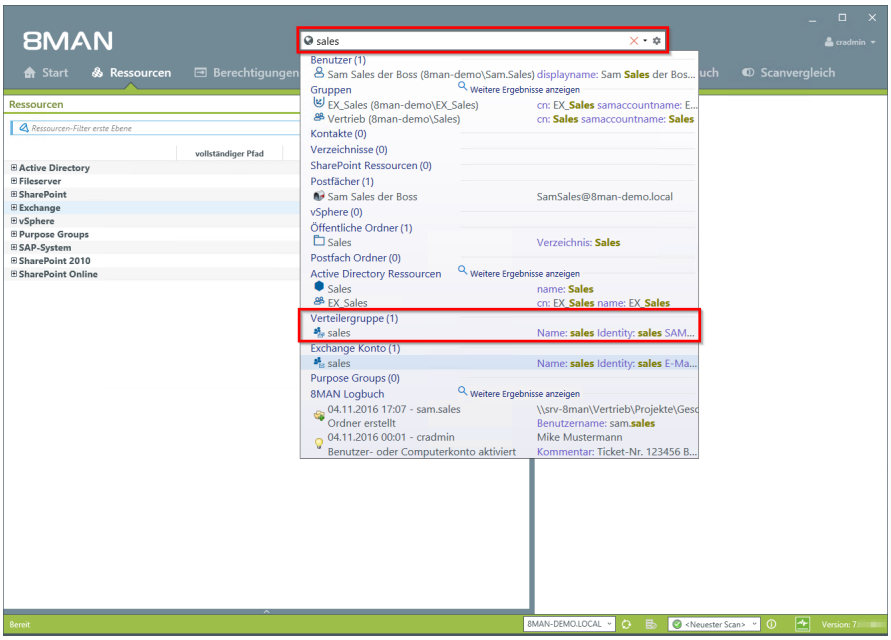
Die Änderung funktioniert auch bei dynamischen Exchange-Gruppen.

Weiterführende Services

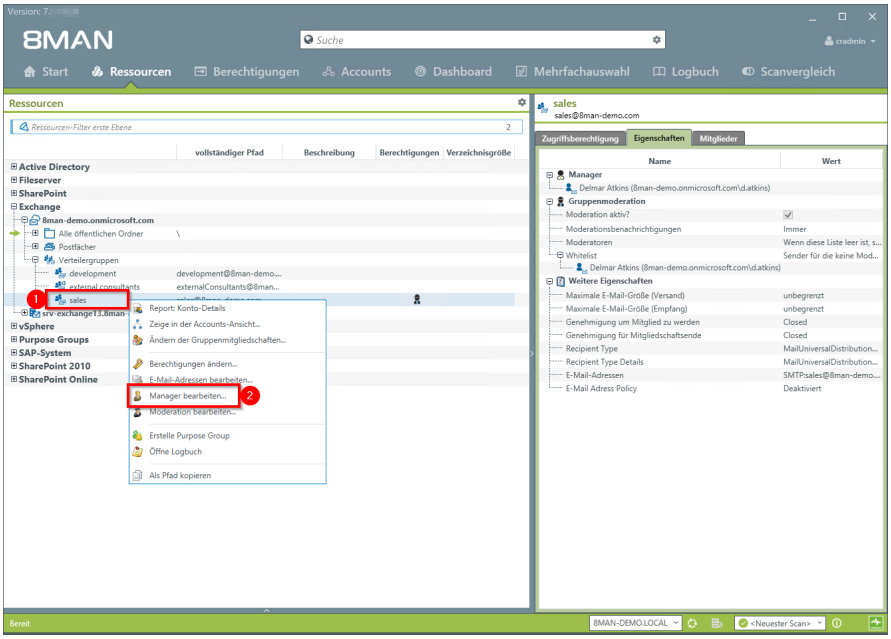
Eigenschaften von Verteilergruppen anzeigen

Moderation von Verteilergruppen ändern

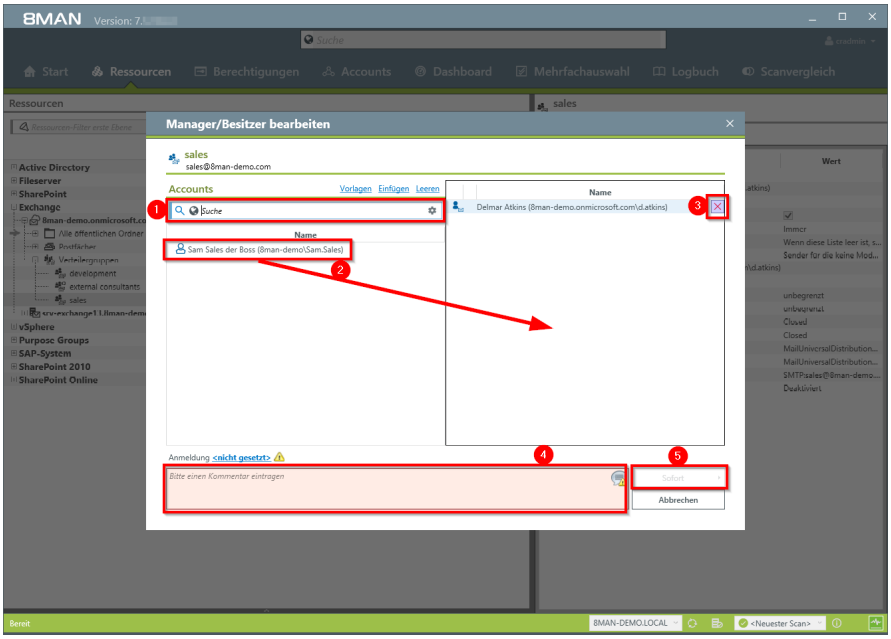
Der Prozess in einzelnen Schritten



Nutzen Sie die Suche, um die gewünschte Verteilergruppe zu finden.



1. *Sie haben die gewünschte Gruppe im Fokus.*
2. *Rechtsklicken Sie auf die Gruppe und wählen "Manager bearbeiten...".*



1. *Nutzen Sie die Suche, um Accounts zu finden. In den Suchoptionen (Zahnrad) muss die Option "Exchange Account" aktiviert sein.*
2. *Ziehen Sie per Drag&Drop Accounts auf die rechte Spalte. Bei dynamischen Verteilergruppen kann im Gegensatz zu Verteilergruppen maximal nur ein Manager existieren.*
3. *Sie können Accounts entfernen.*
4. *Sie müssen einen Kommentar eingeben, z. B. eine Ticketnummer.*
5. *Starten Sie die Ausführung.*

8.3.1.10 Kontakte erstellen und löschen

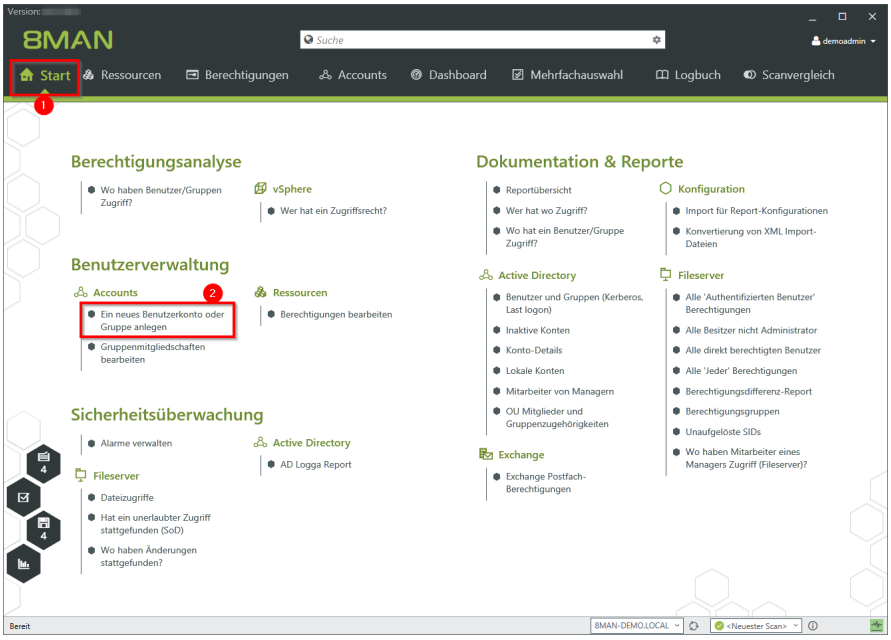
Hintergrund / Mehrwert

Mit 8MAN können Sie dokumentiert Kontakte anlegen und schnell verwalten, z. B. zu Verteilergruppen hinzufügen.

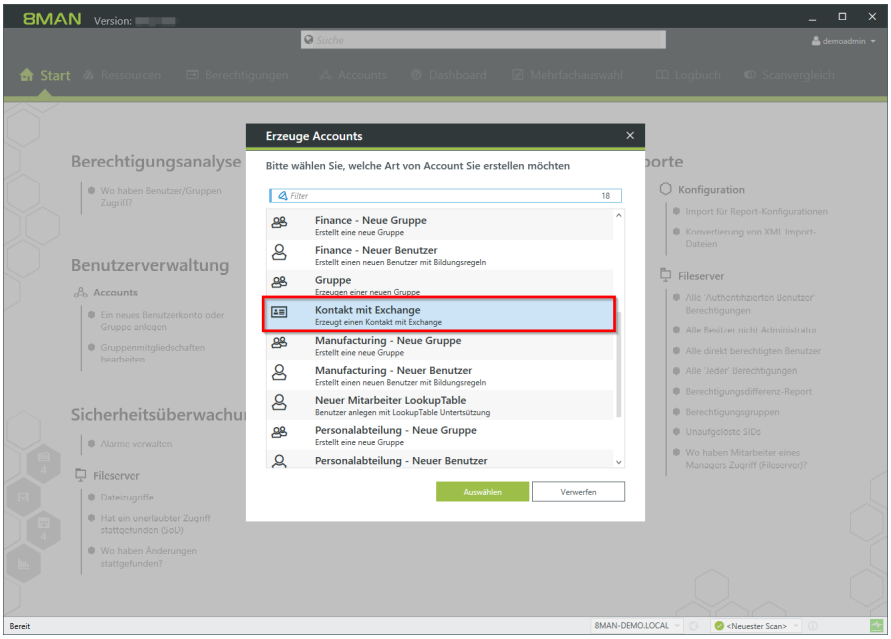
Weiterführende Services

Mitgliedschaften von Verteilergruppen bearbeiten

Der Prozess in einzelnen Schritten



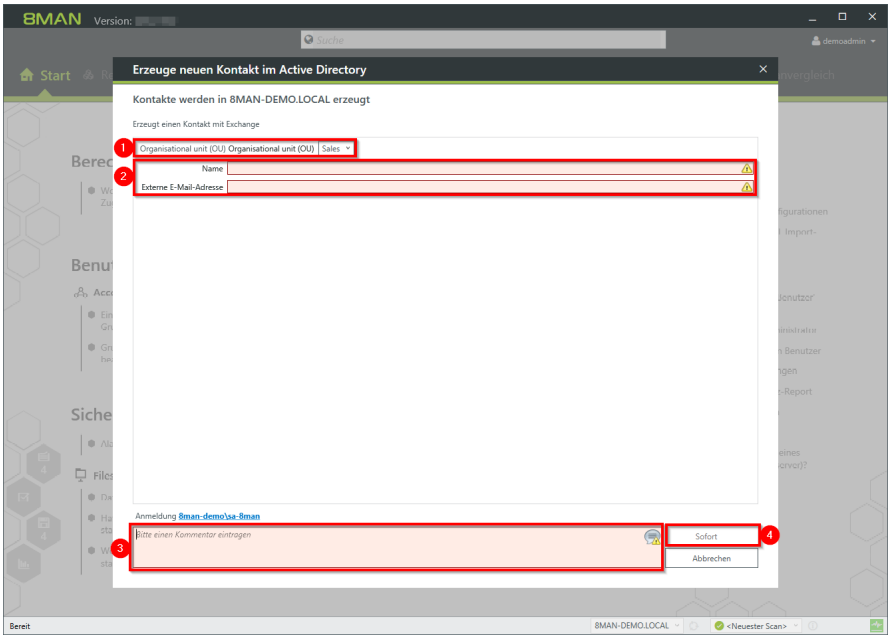
1. *Wählen Sie "Start".*
2. *Klicken Sie auf "Ein neues Benutzerkonto oder Gruppe anlegen".*



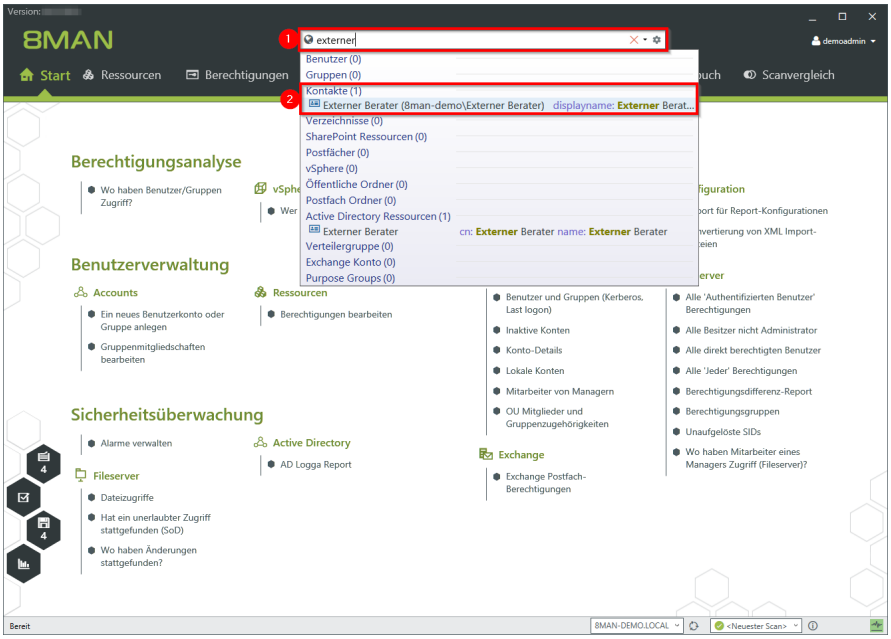
Wählen Sie ein Template zum Erzeugen eines Kontakts aus.

8MAN liefert ein Beispieltemplate für die Anlage von Kontakten. Sie müssen dieses Template anpassen, bevor Sie es verwenden können. Siehe dazu Handbuch Vorlagen anpassen.

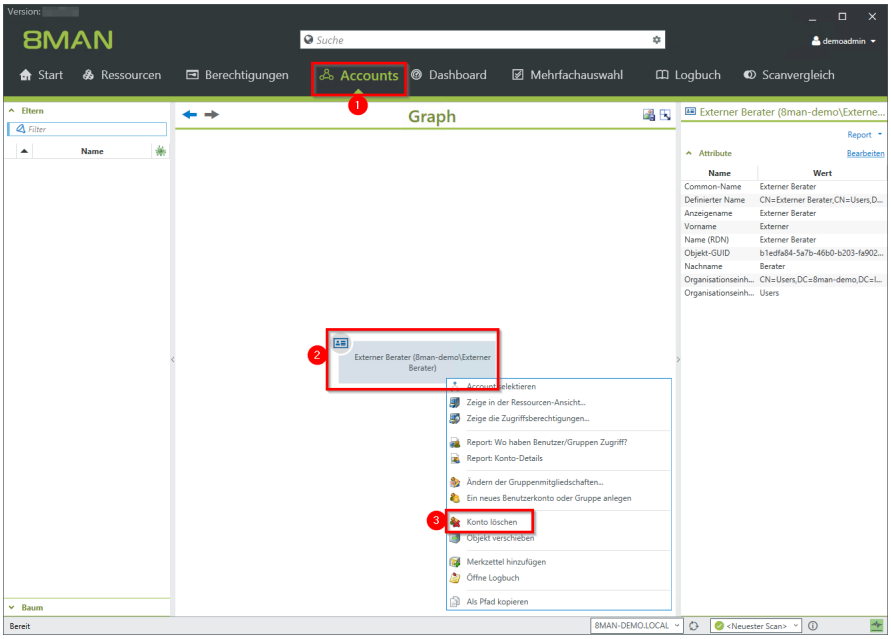
8MAN legt Kontakte mittels Exchange-Powershell-Verbindung an. Eine Lizenz für den 8MATE für Exchange ist erforderlich.



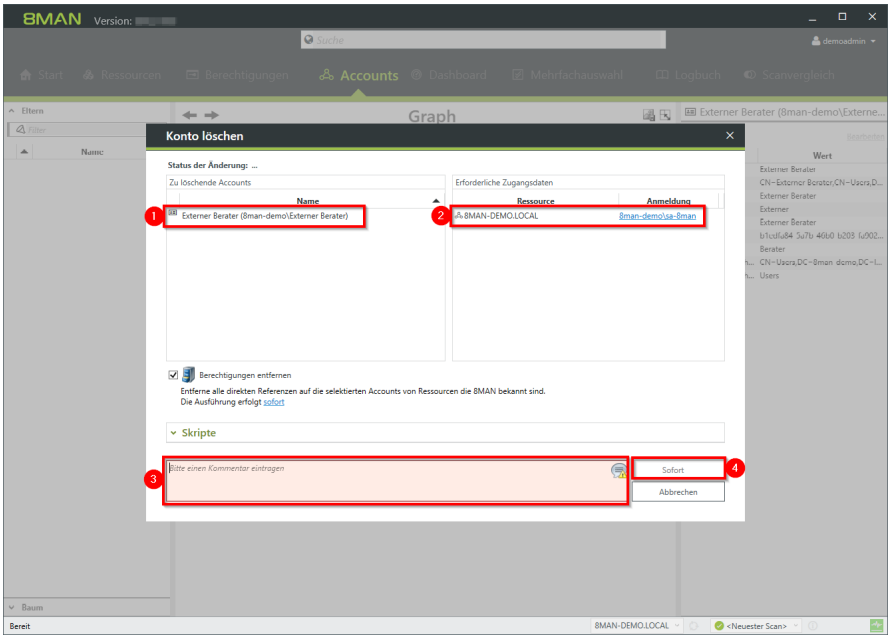
1. *Geben Sie eine OU an.*
2. *Geben Sie Namen und E-Mail-Adressen an.*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie die Ausführung.*



1. *Nutzen Sie die Suche, um einen Kontakt zu finden.*
2. *Klicken Sie auf das Suchergebnis.*



1. *8MAN wechselt in die Accounts-Ansicht.*
2. *Rechtsklicken Sie den Kontakt.*
3. *Wählen Sie Konto löschen.*



1. *8MAN zeigt den zu löschenden Kontakt.*
2. *8MAN zeigt die Anmeldung, mit welcher der Kontakt gelöscht wird. Geben Sie bei Bedarf andere Anmeldeinformationen an.*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie die Ausführung.*

Für das Löschen von Kontakten benötigen Sie keine Exchange-Lizenz.

8.4 +8MATE for SharePoint

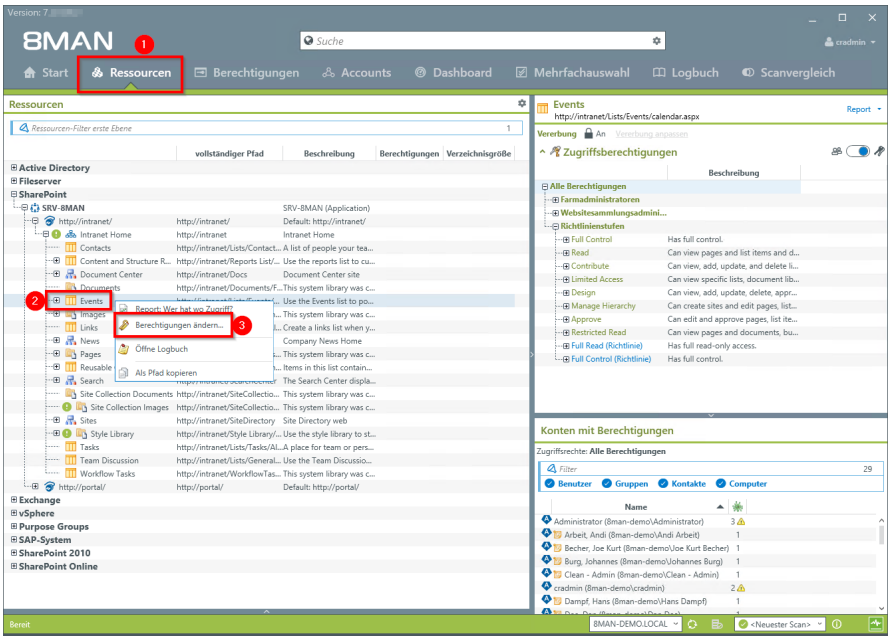
8.4.1 Data Owner

8.4.1.1 Berechtigungen auf SharePoint Ressourcen ändern

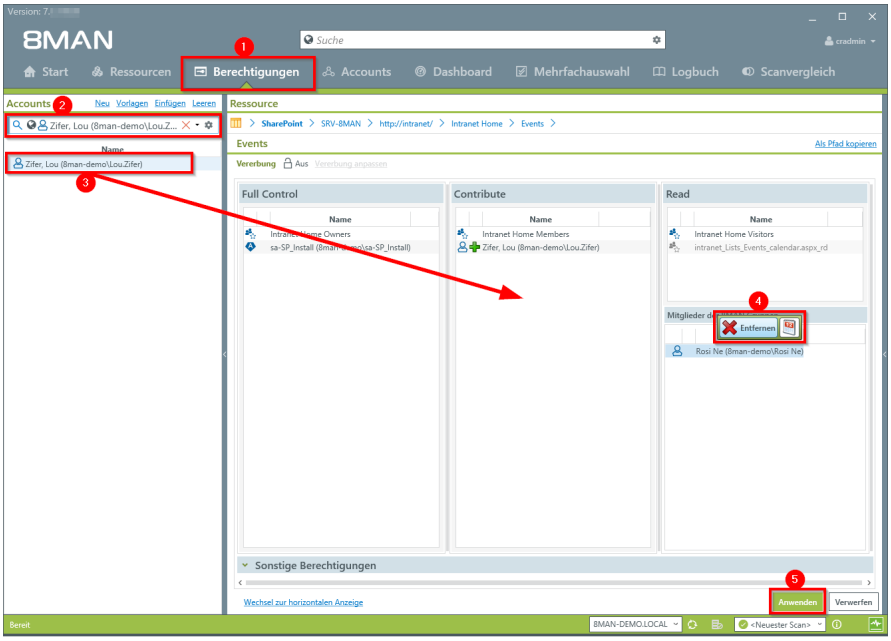
Hintergrund / Mehrwert

Der 8MATE for SharePoint integriert sämtliche SharePoint-Ressourcen in Ihren 8MAN. Damit erfolgt die Analyse zentral und im Einklang mit dem Access Rights Management für andere Anwendungen. Sie profitieren von der Analyse- und Darstellungskompetenz des 8MAN und können Zugangsrechte schnell verändern.

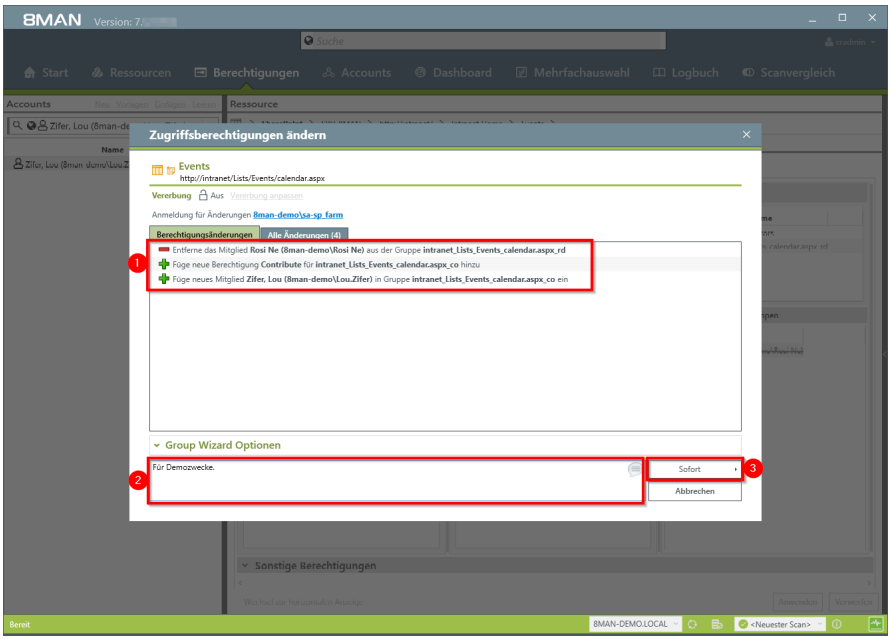
Der Prozess in einzelnen Schritten



1. *Wählen Sie "Ressourcen".*
2. *Navigieren Sie zu der gewünschten Ressource.*
3. *Rechtsklicken Sie auf die Ressource und wählen "Berechtigungen ändern..." im Kontextmenü.*



1. *8MAN wechselt in die Ansicht "Berechtigungen".*
2. *Nutzen sie die Suche, um die gewünschten Accounts zu finden.*
3. *Ziehen sie einen Account per Drag&Drop auf eine Zugriffskategorien-Spalte, um eine Berechtigung zuzuweisen.*
4. *Nutzen sie das Kontextmenü, um einen Benutzer zu entfernen.*
5. *Klicken sie auf "Anwenden".*



1. *Prüfen Sie die geplanten Änderungen.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Starten Sie die Änderung.*

8.4.2 Administrator

8.4.2.1 SharePoint-Gruppen anlegen

Hintergrund / Mehrwert

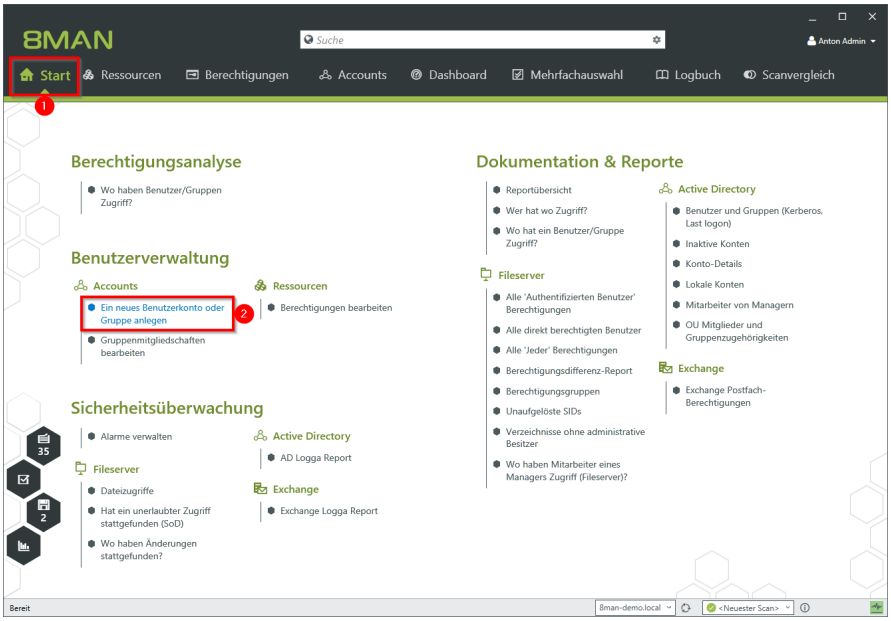
SharePoint-Gruppen können separat vom Active Directory auf einem SharePoint-Server existieren. Erzeugen Sie mit dem SharePoint Remote Connector einfach neue SharePoint-Gruppen.

Nur für den SharePoint Remote Connector (8MATE, der das Client Side Object Model benutzt).

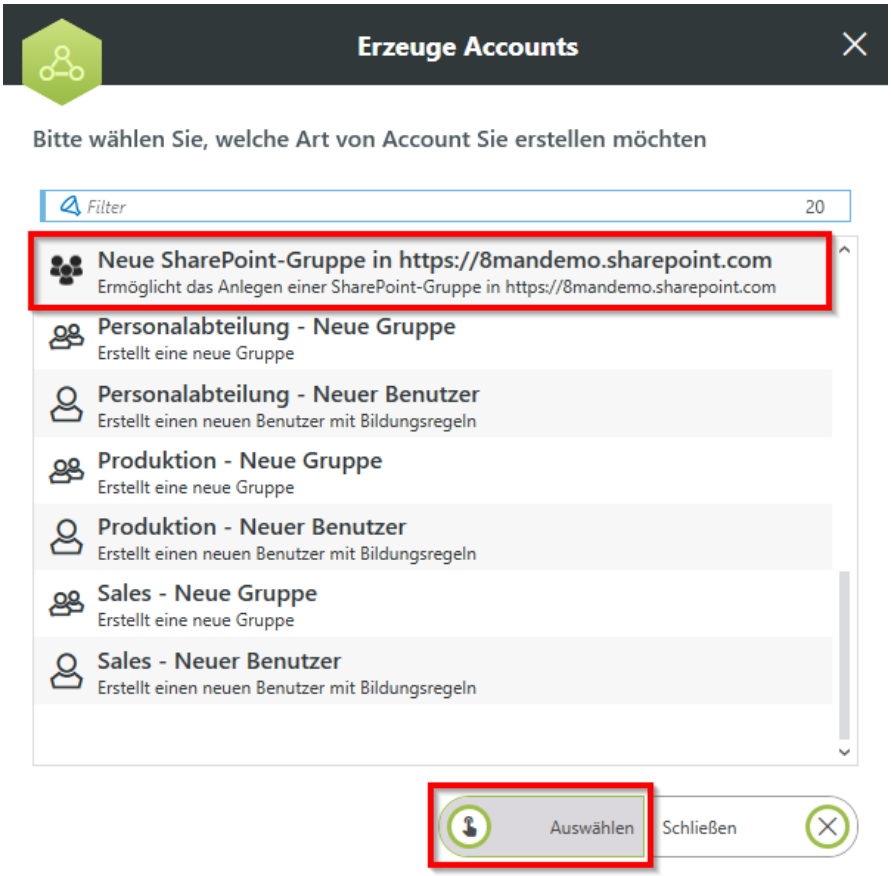
Ähnliche Services

Berechtigungen auf SharePoint Ressourcen ändern

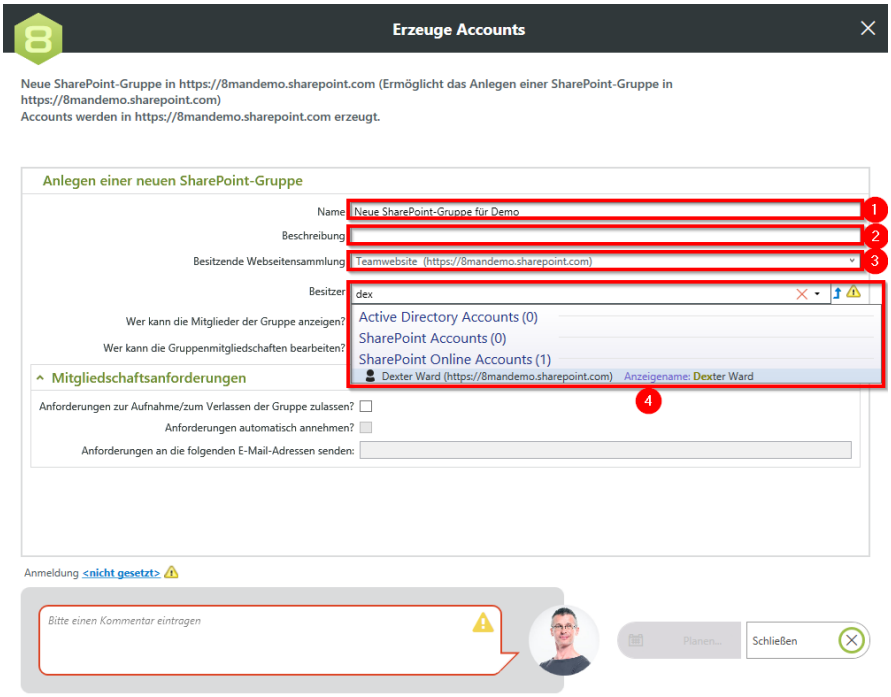
Der Prozess in einzelnen Schritten



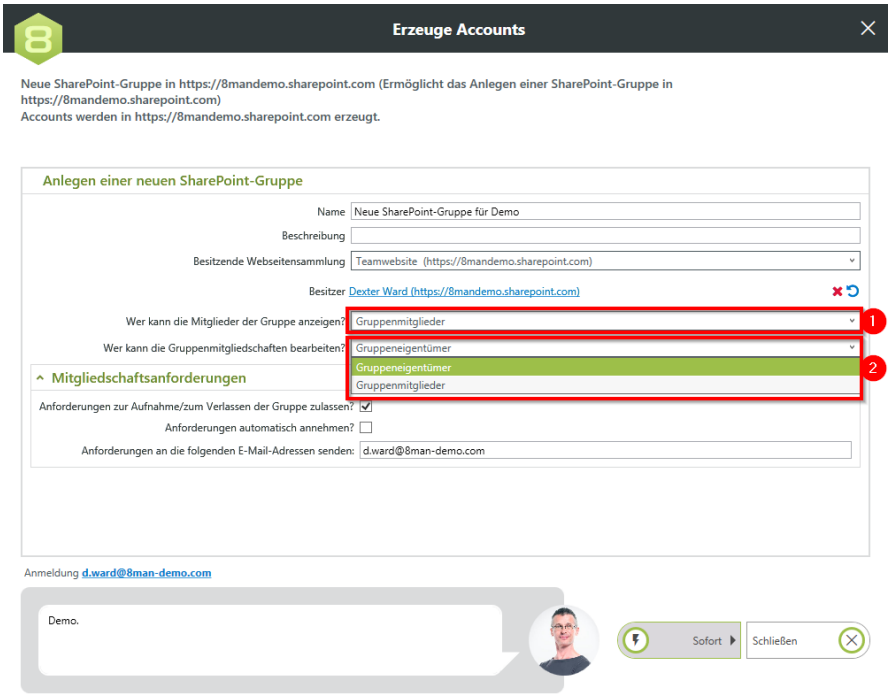
Wählen Sie auf der Startseite "Ein neues Benutzerkonto oder Gruppe anlegen".



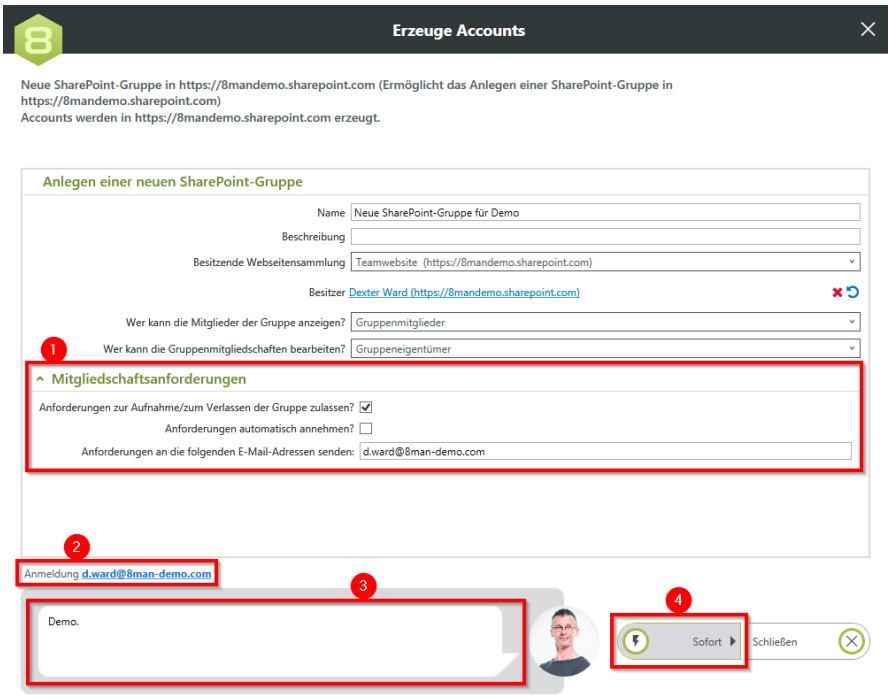
Wählen Sie die Vorlage für die gewünschte SharePoint-Ressource.



1. *Geben Sie einen Namen für die neue Gruppe an.*
2. *Optional: Geben Sie eine Beschreibung an.*
3. *Wählen Sie die Webseitensammlung, der die Gruppe zugeordnet wird.*
4. *Nutzen Sie die Suche, um einen Besitzer festzulegen.*



1. *Wählen Sie aus, wer die Mitglieder der Gruppe sehen darf.*
2. *Wählen Sie aus, wer die Gruppenmitgliedschaften bearbeiten darf.*



1. *Legen Sie fest, wie Mitgliedschaftsanforderungen gehandhabt werden.*
2. *Geben Sie Anmeldeinformationen an, mit denen die neue Gruppe auf SharePoint erzeugt werden darf.*
3. *Sie müssen einen Kommentar angeben.*
4. *Starten Sie die Ausführung.*

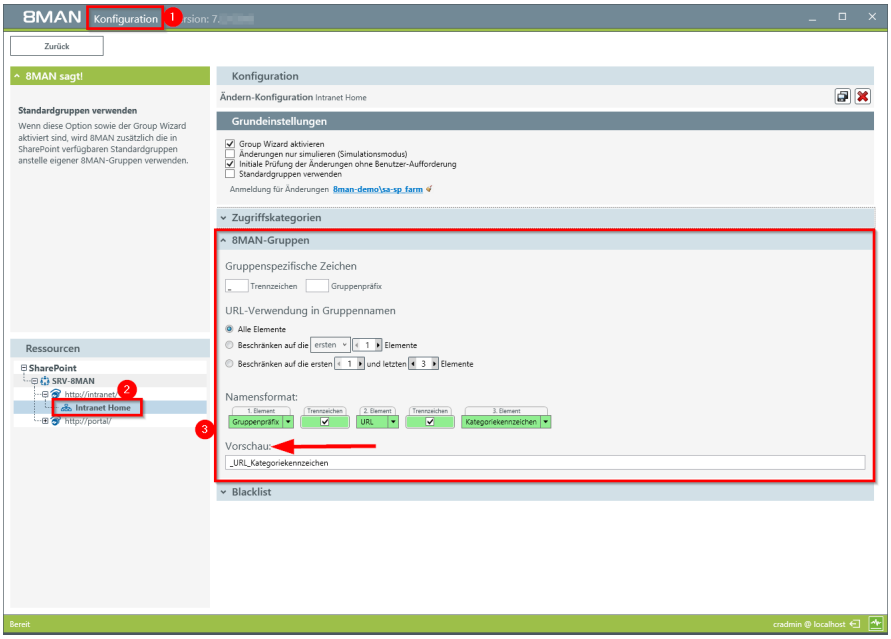
8.4.2.2 Namenskonventionen für Berechtigungsgruppen festlegen

Hintergrund / Mehrwert

8MAN beendet nicht standardisierte Gruppenbezeichnungen. Administratoren einigen sich auf ein Namensschema und die Einhaltung wird bei der Neuerstellung von Berechtigungsgruppen durch 8MAN sichergestellt.

Nur für den 8MATE, der das Server Side Object Model benutzt (nur SharePoint 2010 und 2013).

Der Prozess in einzelnen Schritten



1. *Navigieren Sie in der 8MAN Konfigurationsoberfläche zu "Ändern-Konfiguration" -> "SharePoint".*
2. *Selektieren Sie die gewünschte SharePoint-Ressource. Sie können für jede Ressource spezifische Einstellungen vornehmen.*
3. *Legen Sie die Namenskonventionen fest. Beachten Sie, dass 8MAN Ihnen eine Vorschau anzeigt.*

9. Threat & Gap Management

9.1 +8MATE Clean!

9.1.1 Zu lange Pfade auf dem Fileserver ermitteln

Hintergrund / Mehrwert

Haben Dateien eine Pfadlänge von über 260 Zeichen (inkl. Dateiendung) entstehen Probleme:

Programme können auf diese Dateien nicht mehr zugreifen und somit sind sie weder kopier-, bearbeit- oder löschbar. 8MATE Clean! zeigt alle Dateien mit zu langen Pfaden.

Wir empfehlen, die Ordnernamen zu kürzen und/oder die betroffenen Verzeichnisse auf eine höhere Ebene zu verschieben.

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.

Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.2 Alte Fileserver Dateien archivieren

Hintergrund / Mehrwert

Access Rights Management bedeutet auch alte, nicht mehr benutzte Daten zu archivieren. Denn: Je geringer die Datenmasse, desto einfacher deren Verwaltung und geringer die Kosten. Der 8MATE Clean! erlaubt Ihnen ab einem bestimmten Datum Dateien als „alt“ zu markieren. Es gilt, als maßgeblicher Parameter, der letzte Schreib- oder Lesezugriff.

Entscheiden Sie anschließend, ob die Dateien auf ein anderes Zielsystem verschoben werden sollen, oder im Rahmen einer Fileserver-Migration auf dem alten System verbleiben.

Weiterführende Services

Wollen Sie die alten Dateien archivieren, empfehlen wir vorher mit 8MAN einen geschützten Bereich anzulegen und die zu archivierenden Dateien dort abzulegen:

Anwenderhandbuch: Einen geschützen Bereich auf dem Fileserver anlegen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.3 Die Zugriffsrechte auf leere Unterordner vererben

Hintergrund / Mehrwert:

Leere Ordner brauchen keine abweichenden Berechtigungen. Der 8MATE Clean! entfernt diese, indem die Rechte von übergeordneten Ordnern vererbt werden. Dadurch wird die Berechtigungssituation auf dem Fileserver harmonisiert.

Alternativer Service:

Leere Ordner auf dem Fileserver löschen (8MATE Clean!)

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.4 Leere Fileserver-Verzeichnisse löschen

Hintergrund / Mehrwert:

Leere Ordner können Sie automatisch löschen lassen. Dadurch wird die Struktur bereinigt.

Alternativer Service:

Sind Sie nicht sicher, ob leere Ordner bewusst angelegt wurden, nutzen Sie den folgenden Service:
8MATE Clean! Handbuch: Die Zugriffsrechte auf leere Unterordner vererben

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.5 Nicht kanonische Berechtigungen korrigieren

Hintergrund / Mehrwert

Die Zugriffsberechtingungsseinträge (Access Control Entries, ACEs) haben je nach Typ eine bestimmte Reihenfolge in der DACL. Konkret stehen ACEs, die den Zugriff verweigern vor ACEs, die den Zugriff gewähren. Die Reihenfolge der ACEs entscheidet über das effektive Zugriffsrecht des Nutzers. Durch ACEs in falscher Reihenfolge entstehen Sicherheitsrisiken.

8MATE Clean! repariert die nicht kanonischen Berechtigungen und stellt den Standard wieder her.

Alternative Services

Nicht kanonische Berechtigungen durch übergeordnete Rechte ersetzen (8MATE Clean!)

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.6 Nicht kanonische Berechtigungen durch übergeordnete Rechte ersetzen

Hintergrund / Mehrwert

Die Zugriffsberechtingungsseinträge (Access Control Entries, ACEs) haben je nach Typ eine bestimmte Reihenfolge in der DACL. Konkret stehen ACEs, die den Zugriff verweigern vor ACEs, die den Zugriff gewähren. Die Reihenfolge der ACEs entscheidet über das effektive Zugriffsrecht des Nutzers. Durch ACEs in falscher Reihenfolge entstehen Sicherheitsrisiken.

8MATE Clean! beseitigt die nicht kanonische Berechtigung, indem die DACL des darüber liegenden Verzeichnisses vererbt wird.

Alternativer Service

Möchten Sie sicherstellen, dass etwaige Berechtigungsdifferenzen zwischen Ober- und Unterordner bestehen bleiben nutzen Sie folgenden Service:

Nicht kanonische Berechtigungen korrigieren

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.7 Kritische Berechtigungen automatisiert ersetzen

Hintergrund / Mehrwert

Es gibt eine Reihe von Gruppen und Konten in der DACL, die auf keinen Fall Berechtigungen bekommen sollten. Dazu zählen z.B. der EVERYONE oder der CREATOR/OWNER Accounts. Die eben genannten kritischen Accounts, aber auch spezielle Windows Accounts sind in der 8MAN Blacklist definiert und können mit 8MAN nicht berechtigt werden.

Wurden ohne 8MAN kritische Berechtigungen gesetzt, kann der 8MATE Clean! diese automatisch für Sie ersetzen. Sie definieren, welche Gruppen und Direktberechtigungen durch welche Berechtigungen ersetzt werden sollen und der 8MATE Clean! setzt Ihre Anforderungen um.

Alternative Services

8MATE Anwenderhandbuch: Kritische Berechtigungen automatisiert entfernen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.8 Null DACLs identifizieren und durch übergeordnete Berechtigungen ersetzen

Hintergrund / Mehrwert:

Der Security Descriptor einer DACL kann bei Verzeichnissen den Wert "0" aufweisen. In diesem Fall kann sich jeder den gewünschten Zugriff auf die darin enthaltenen Unterverzeichnisse und Dateien selbst besorgen. Null DACLs entstehen durch fehlerhafte Applikationen, welche die ACL's manipulieren.
Der 8MATE Clean! ersetzt die Null DACL durch übergeordnete Berechtigungen.

Hinweis: Der Service ist nur für Windows Fileserver relevant. Bei NetAPP und EMC Servern können Null DACLs nicht auf dem Share ersetzt werden. Sie finden dort standardmäßig Verwendung.

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.9 Abweichende Berechtigungsarten auf dem Fileserver ersetzen

Hintergrund / Mehrwert

Zugriffskategorien bestimmen die Art und Weise wie zugegriffen werden kann. In 8MAN ist die Auswahl auf praxistaugliche Kategorien eingegrenzt. Dazu zählen "Vollzugriff", "Ändern", "Lesen und Ausführen" , "Schreiben" und "Ordnerinhalte anzeigen bzw. auflisten". Microsoft erlaubt hingegen eine Vielzahl von Zugriffskategorien. Insbesondere "Spezielle Rechte" verkomplizieren durch ihre Granularität und freie Kombinierbarkeit die Rechtevergabe unnötig. Die Protected Networks GmbH empfiehlt mit lediglich drei Zugriffskategorien zu arbeiten:

- Vollzugriff
- Ändern
- Lesen und Ausführen

Mit dem 8MATE Clean! können Sie die vorhandene Rechtestruktur automatisch und nach Ihren Wünschen umwandeln lassen. Dadurch vereinfachen Sie signifikant das Rechte-Management auf Ihren Fileservern.

Weiterführende Services

Ändern Sie passend zum Soll Zustand, die Konventionen für die Erstellung von neuen Berechtigungen:

8MAN Installation und Konfiguration: Die in 8MAN verfügbaren Zugriffskategorien wählen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.10 Abweichende Berechtigungsarten löschen

Hintergrund / Mehrwert

Zugriffskategorien bestimmen die Art und Weise wie zugegriffen werden kann. In 8MAN ist die Auswahl auf praxistaugliche Kategorien eingegrenzt. Dazu zählen "Vollzugriff", "Ändern", "Lesen und Ausführen" , "Schreiben" und "Ordnerinhalte anzeigen bzw. auflisten". Microsoft erlaubt eine Vielzahl von Berechtigungsarten. Insbesondere "Spezielle Rechte" verkomplizieren durch ihre Granularität und freie Kombinierbarkeit die Rechtevergabe unnötig . Die Protected Networks GmbH empfiehlt mit lediglich drei Rechten zu arbeiten:

- Vollzugriff
- Ändern
- Lesen und Ausführen

Mit dem 8MATE Clean! können Sie die ungewollten Berechtigungsarten löschen.
Dann verlieren alle Nutzerkonten die ausschließlich über die gelöschten Berechtigungen Zugriff hatten, ihren Zugriff auf die betroffenen Verzeichnisse.

Weiterführende Services

Der 8MATE Clean! erlaubt die bereits gesetzten Rechte entsprechend ihrer Vorgaben zu ersetzen:

8MATE Clean! Handbuch: Abweichende Berechtigungsarten ersetzen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.11 Kritische Berechtigungen automatisch entfernen

Hintergrund / Mehrwert:

Es gibt eine Reihe von Gruppen und Konten in der DACL, die auf keinen Fall Berechtigungen bekommen sollten. Dazu zählen z.B. der EVERYONE oder der CREATOR/OWNER Accounts. Die eben genannten kritischen Accounts, aber auch spezielle Windows Accounts sollten nicht berechtigt werden.

Wurden ohne 8MAN kritische Berechtigungen gesetzt, kann der 8MATE Clean! diese automatisch für Sie entfernen.

Alternative Services:

8MATE Clean! Handbuch: Kritische Berechtigungen automatisiert ersetzen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.12 Direktberechtigungen löschen

Hintergrund / Mehrwert

Direktberechtigungen sind ineffizient, weil jeder Nutzer einzeln berechtig werden muss. Direktberechtigungen verursachen nach Löschung des Nutzerkontos sog. verwaiste SIDs. Mit diesen kann sich ein anderer Nutzer Zugriff verschaffen. Direktberechtigungen verlängern die ACL auf dem Fileserver und damit auch die Dauer der Überprüfung, ob ein Benutzer den angeforderten Zugriff bekommt. Sie sollten vermieden werden und durch Berechtigungen über Gruppen ersetzt oder gelöscht werden.

8MATE Clean! identifiziert alle Direktberechtigungen auf Ihren Fileservern und löscht diese.

Alternative Services:

Sollen die Konten mit Direktberechtigungen trotzdem noch Zugriff haben, empfehlen wir das Ersetzen der Direktberechtigungen:

8MATE Clean! Handbuch: Direktberechtigungen durch Gruppenmitgliedschaften ersetzen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.13 Direktberechtigungen durch Gruppenmitgliedschaften ersetzen

Hintergrund / Mehrwert

Direktberechtigungen sind ineffizient, weil jeder Nutzer einzeln berechtig werden muss. Sie sollten vermieden werden und durch Berechtigungen über Gruppen ersetzt werden.
Darüber hinaus muss jedes Verzeichnis bei der Rechteentfernung gesondert geprüft werden. 8MATE Clean! identifiziert alle Direktberechtigungen auf Ihren Fileservern und wandelt diese in Gruppenberechtigungen um.

Die Umwandlung von Direktberechtigungen hat folgende Vorteile:
Direktberechtigungen verursachen nach Löschung des Nutzerkontos sog. verwaiste SIDs. Mit diesen kann sich ein anderer Nutzer Zugriff verschaffen. Direktberechtigungen verlängern die ACL auf dem Fileserver und damit auch die Dauer der Überprüfung, ob ein Benutzer den angeforderten Zugriff bekommt.

Alternative Services:

Sollen die Konten mit Direktberechtigungen keine Zugriff mehr haben, empfehlen wir das Löschen der Direktberechtigungen.

8MATE Clean! Handbuch: Direktberechtigungen löschen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.14 Bei identischen Ordner-Berechtigungen die Vererbung aktivieren

Hintergrund / Mehrwert:

Manchmal verfügen Verzeichnisse in einem Baum über die gleichen Berechtigungen, aber die Vererbung ist trotzdem deaktiviert. 8MATE Clean! identifiziert diese Verzeichnisse und aktiviert die Vererbung. Dies vereinfacht das Berechtigungsmanagement, da spätere, in den übergeordneten Verzeichnissen gemachte Berechtigungsänderungen sich auf darunterliegende Verzeichnisse übertragen.

Weiterführende Services:

Um die Kerberos-Token Belastung weiter zu senken, empfehlen wir den folgenden Services:

8MATE Clean Handbuch: Leere Ordner auf dem Fileserver löschen

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.15 Berechtigungsunterbrechungen durch Angleichung der Verzeichnis Owner aufheben

Hintergrund / Mehrwert

Nur Administratoren sollten nach Microsoft Best Practice Besitzer eines Verzeichnisses sein. Dieses Recht sollte nur Administratoren vorbehalten sein, da Besitzer automatisch Vollzugriff haben. 8MATE Clean! ersetzt abweichende Verzeichnis Owner wieder durch den Administrator.

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

9.1.16 Die Berechtigungstiefe auf Fileservern automatisch vermindern

Hintergrund / Mehrwert

In der 8MAN Konfiguration ist die maximale Berechtigungstiefe ab Share definiert. Davon abweichende Berechtigungen, betrachtet 8MAN als „zu tiefe Berechtigungen“.
8MAN Clean! ersetzt abweichende Berechtigungen ab dem laut Definition zulässigen Maximalwert durch die Berechtigungen der übergeordneten Ordner.

Die Harmonisierung der Berechtigungssituation ab einer bestimmten Tiefe hat den Sinn, die Komplexität der Ordnerverwaltung einzuschränken. Dadurch verringern sich Aufwände in der IT.

8MATE Clean! wird durch unsere erfahrenen System Engineers ausgeführt.
Kontaktieren Sie uns, um weitergehende Informationen zu erhalten: info@8man.com

10. 8MAN Application Integration

10. +8MATE Matrix 42 1

10.1.1 Für Mitarbeiter

10.1.1.1 Fileserver Berechtigungen bestellen

Bitte wenden Sie sich an das Knowledge Management, um weitere Informationen zu erhalten.

KM@8MAN.com

10.1.2 Für Data Owner und Administratoren

10.1.2.1 Eine Anfrage umsetzen lassen oder ablehnen

Bitte wenden Sie sich an das Knowledge Management, um weitere Informationen zu erhalten.

KM@8MAN.com

11. Anhang

11. Software-Lizenzvereinbarungen 1

- Json.net, © 2006-2014 Microsoft, https://json.codeplex.com/license
- JSON.NET Copyright (c) 2007 James Newton-King https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md
- Irony Copyright (c) 2011 Roman Ivantsov http://irony.codeplex.com/license
- Jint Copyright (c) 2011 Sebastien Ros http://jint.codeplex.com/license
- #ziplib 0.85.5.452, © 2001-2012 IC#Code, http://www.icsharpcode.net/opensource/sharpziplib/
- PDFsharp 1.33.2882.0, © 2005-2012 empira Software GmbH, Troisdorf (Germany), http://www.pdfsharp.net/PDFsharp_License.ashx
- JetBrains Annotations, ©2007-2012 JetBrains, http://www.apache.org/licenses/LICENSE-2.0
- Microsoft Windows Driver Development Kit, © Microsoft, EULA, installed on the computer on which the FS Logga for Windows file servers is installed: C:\Program Files\protected-networks.com\8MAN\driver (Usage only for FS Logga for Windows file server)
- NetApp Manageability SDK, © 2013 NetApp, https://communities.netapp.com/docs/DOC-1152 (Usage only for FS Logga for NetApp Fileserver)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation , http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx
- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, http://wpf.codeplex.com/license
- WpfAnimatedGif, © Copyright 2012-2017 Thomas Levesque, https://github.com/XamlAnimatedGif/WpfAnimatedGif/blob/master/LICENSE.txt
- Bootstrap, © 2011-2016 Twitter, Inc, https://github.com/twbs/bootstrap/blob/master/LICENSE
- jQuery, © 2016 The jQuery Foundation, https://jquery.org/license
- jquery.cookie, © 2014 Klaus Hartl, https://github.com/carhartl/jquery-cookie/blob/master/MIT-LICENSE.txt
- jquery-tablesort, © 2013 Kyle Fox, https://github.com/kylefox/jquery-tablesort/blob/master/LICENSE
- LoadingDots, © 2011 John Nelson, http://johncoder.com
- easyModal.js, © 2012 Flavius Matis, https://github.com/flaviusmatis/easyModal.js/blob/master/LICENSE.txt
- jsTimezoneDetect, © 2012 Jon Nylander https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENCE.txt?at=defaultjquery-tablesort
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community https://github.com/janl/mustache.js/blob/master/LICENSE
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE
- Underscore.js, © 2009-2016 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors https://github.com/jashkenas/underscore/blob/master/LICENSE

- Ractive.js, © 2012-15 Rich Harris and contributors, https://github.com/ractivejs/ractive/blob/dev/LICENSE.md
- RequireJS, © 2010-2015, The Dojo Foundation, https://github.com/jrburke/requirejs/blob/master/LICENSE
- typeahead.js, © 2013-2014 Twitter, Inc, https://github.com/twitter/typeahead.js/blob/master/LICENSE
- Select2, © 2012-2015 Kevin Brown, Igor Vaynberg, and Select2 contributors https://github.com/select2/select2/blob/master/LICENSE.md
- bootstrap-datepicker, © Copyright 2013 eternicode https://github.com/eternicode/bootstrap-datepicker/blob/master/LICENSE
- RabbitMQ, © Copyright 2007-2013 GoPivotal, https://www.rabbitmq.com/mpl.html
- EPPlus, JanKallman, https://github.com/JanKallman/EPPlus/blob/master/LICENSE

8

A

B

C

D

E

F

G

H

I

J

K

L

M

O

P

R

S

U

V

W

Z