8MAN

Access Rights Management. Only much Smarter.

Access Rights Management

Release Notes

Version 9

Protected Networks

1 Editorial

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 2017 haben wir mit über 1.000 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 bedanken wir uns recht herzlich bei Ihnen und wünschen viel Spaß mit dem Release 9!

Zu den Highlights zählen die neuen Cockpits, Nutzerprofile, der 8MATE Exchange Logga und die Alerts für FS Logga Ereignisse.

Berlin im Januar 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
Knowledgebase

Redaktion

Fabian Fischer
Jörg Brandt

Stephan Brack
CEO Protected Networks

Matthias Schulte-Huxel
CSO Protected Networks

2 Das Release nach Produktgruppen

9.0	8MAN Visor	8MAN Visor DO	8MAN Enterprise
Übergreifende Änderungen			
User Cockpits: Solutions for People	✓	✓	✓
Security Monitoring			
Exchange Aktivitäten überwachen	8MATE Exchange Logga	8MATE Exchange Logga	8MATE Exchange Logga
Alarme für Fileserver	8MATE FS Logga	8MATE FS Logga	8MATE FS Logga
Role & Process Optimization			
Skriptbasierte Services im GrantMA Self-Service-Portal bestellen	✗	✗	8MATE GrantMA
Zu rezertifizierende Ressourcen festlegen	✗	✗	✓
Benachrichtigungs-E-Mails für die Rezertifizierung testen	✗	✗	✓
User Provisioning			
8MAN Abteilungsprofile und Compliance Check	✗	✗	✓
Computerkonten editieren	✗	✗	✓
Computerkonten löschen	✗	✗	✓
Resource Integration			
Dynamics NAV Berechtigungen analysieren	8MATE for Dynamics NAV	8MATE for Dynamics NAV	8MATE for Dynamics NAV
8MAN Konfiguration			
Farbanpassung des Setups	✓	✓	✓

3 Übergreifende Änderungen

3.1 User Cockpits: Solutions for People

Access Rights Management ist nicht nur ein Thema für Administratoren. Um Ressourcen im Firmennetzwerk effizient abzusichern, muss Sicherheitskompetenz dezentralisiert werden. Deshalb erweitert die Protected Networks GmbH ihr Referenzprodukt 8MAN um individuelle Cockpits.

In folgenden Tabelle finden Sie die für die Rollen maximal verfügbaren Services im Cockpit. In der 8MAN Konfiguration legen Sie fest, welche Services für welche Rollen verfügbar sind.

	Admin	HelpDesk	DataOwner	Auditor	Manager	Mitarbeiter
Risiken minimieren						
Nonkonforme Benutzer identifizieren	✓	✓	✓	✗	✓	✗
Bestellungen verwalten						
Meine Bestellungen verwalten	✓	✓	✓	✓	✓	✓
Bestellanfragen genehmigen oder ablehnen	✓	✓	✓	✗	✓	✗
Benutzeraktionen ausführen						
Kennwörter zurücksetzen	✓	✓	✓	✗	✓	✗
Benutzer pausieren	✓	✓	✓	✗	✓	✗
Kontodaten von Benutzern ändern	✓	✓	✓	✗	✗	✗
Benutzer deaktivieren	✓	✓	✓	✗	✗	✗
Einen neuen Benutzer anlegen	✓	✓	✓	✗	✗	✗
Benutzern ein Abteilungsprofil zuweisen	✓	✓	✓	✗	✓	✗
Gruppenaktionen ausführen						
Mitgliedschaften entfernen	✓	✓	✓	✗	✗	✗
Mitgliedschaften hinzufügen	✓	✓	✓	✗	✗	✗
Mein Bereich						
Die eigenen Kontodaten ändern	✓	✓	✓	✓	✓	✓
Meine Mitarbeiter	✓	✓	✓	✗	✓	✗

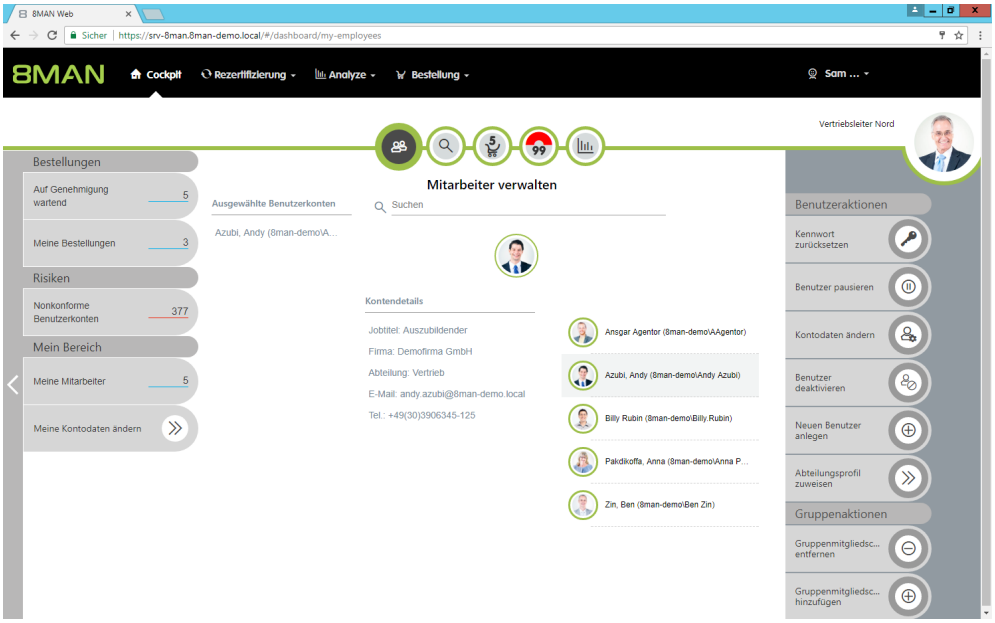
3.1.1 Das Manager Cockpit: Die Sicherheitskompetenz von Führungskräften stärken

Access Rights Management ist nicht nur ein Thema für Administratoren. Um Ressourcen im Firmennetzwerk effizient abzusichern, muss Sicherheitskompetenz dezentralisiert werden. Wer auf welche Ressourcen zugreifen kann, ist Chefsache. Deshalb erweitert die Protected Networks GmbH ihr Referenzprodukt 8MAN um ein Manager Cockpit.

Mit Hilfe einer einfachen Übersicht kann jede Führungskraft im Unternehmen ihren Beitrag für mehr Datensicherheit leisten und Mitarbeiter und deren Berechtigungen verwalten.

Services

Übersicht aller Cockpit-Services



Beispiel für ein Manager Cockpit.

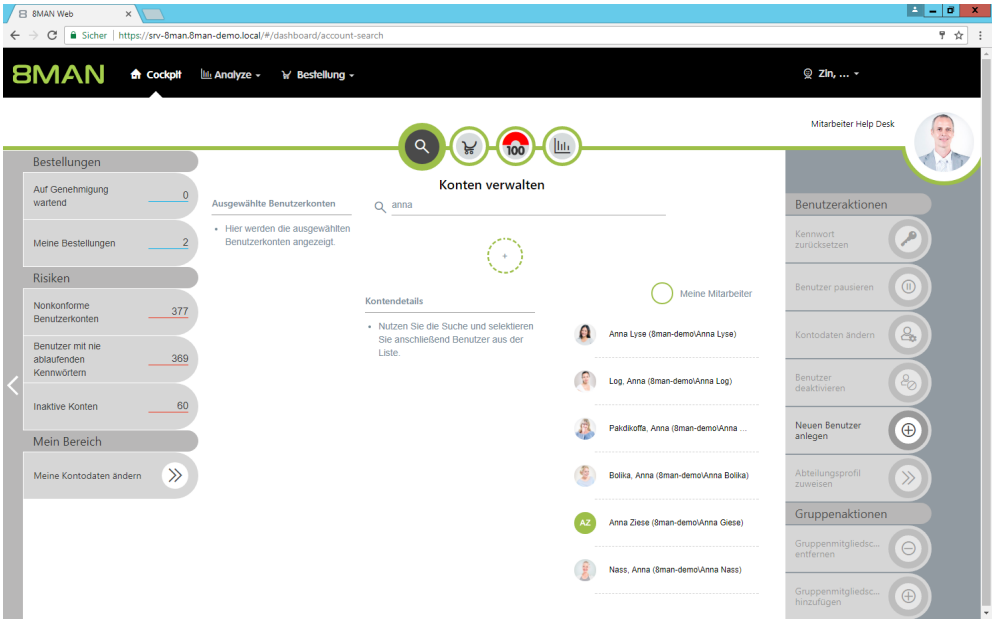
Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login) und Konfiguration.

3.1.2 Das Help Desk Cockpit: Klare, einfache Prozesse für den Support

Access Rights Management läuft effizient, wenn Standardoperationen delegierbar sind. Ob über unser eigenes Bestellportal oder die Anbindung eines Ticketsystems. Mit 8MAN erhalten Helpdesk Mitarbeiter klare Aufgaben und einfache Prozesse. Die Folge: Der Administrator wird entlastet und kann sich um seine Infrastruktur-Projekte kümmern.

Services

Übersicht aller Cockpit-Services



Beispiel für ein HelpDesk Cockpit.

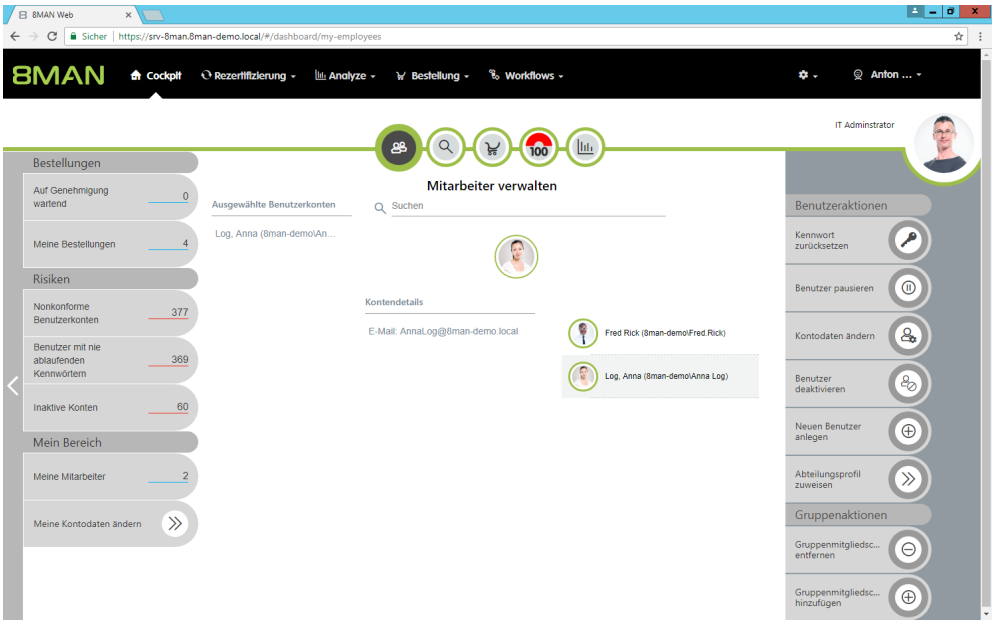
Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login) und Konfiguration.

3.1.3 Das Administrator Cockpit

Zahlreiche Administratorfunktionen, darunter viele Bulk-Operations, stehen jetzt im Webclient zur Verfügung.

Services

Übersicht aller Cockpit-Services



Beispiel für ein Administrator Cockpit.

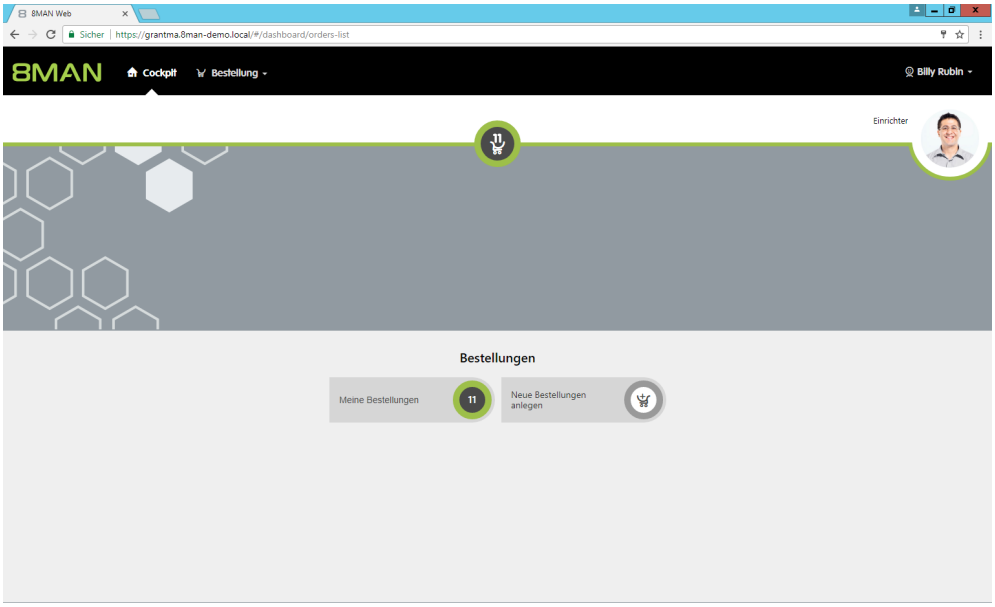
Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login) und Konfiguration.

3.1.4 Das Mitarbeiter Cockpit

Access Rights Management ist nicht nur ein Thema für Administratoren. Um Ressourcen im Firmennetzwerk effizient abzusichern, muss Sicherheitskompetenz dezentralisiert werden. Deshalb erweitert die Protected Networks GmbH ihr Referenzprodukt 8MAN um ein Mitarbeiter Cockpit.

Services

Übersicht aller Cockpit-Services



Beispiel für ein Mitarbeiter Cockpit.

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

3.1.5 Alle Cockpit-Services

3.1.5.1 Bestellungen

3.1.5.1.1 Meine Bestellungen verwalten (Cockpit)

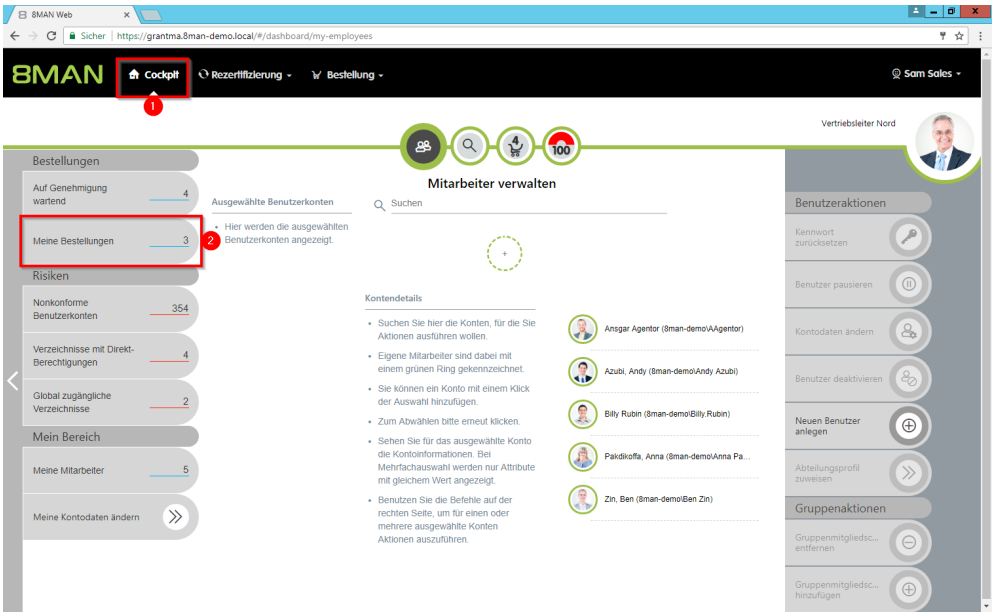
Hintergrund / Mehrwert

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

Weiterführende Services

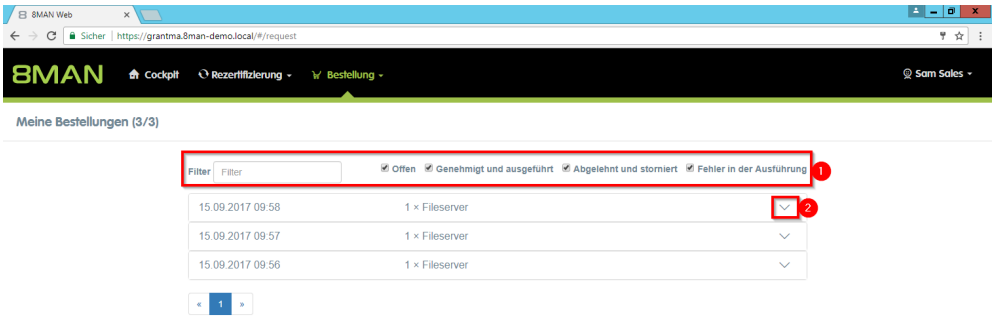
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

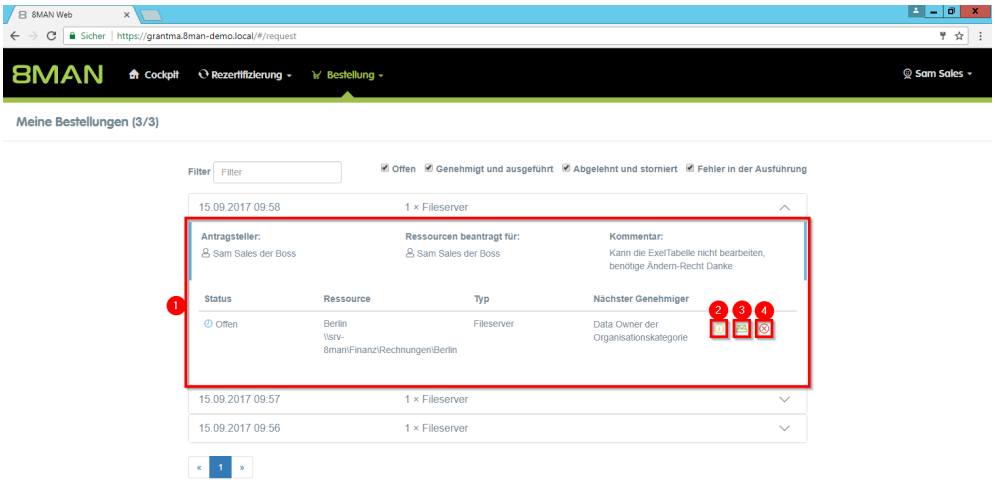


1. *Wählen Sie Cockpit.*
2. *Klicken Sie auf meine Bestellungen. In dem Beispiel hat Sam Sales "3" Bestellungen.*

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.*

3.1.5.1.2 Bestellungen genehmigen oder ablehnen (Cockpit)

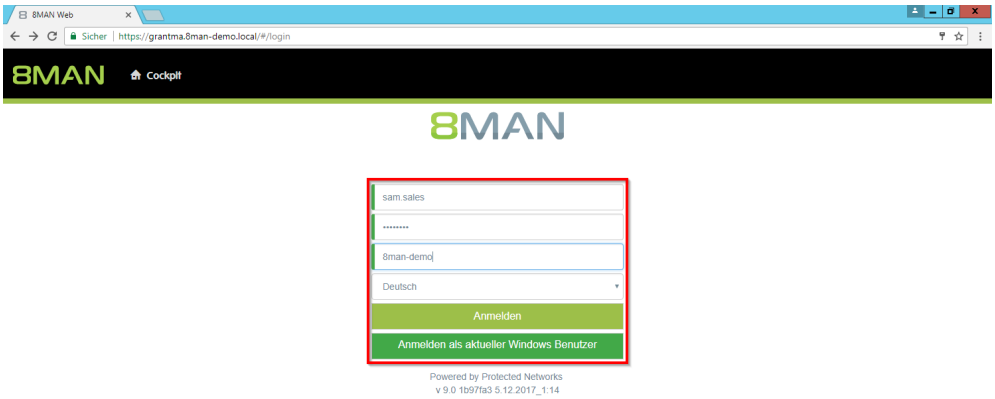
Hintergrund / Mehrwert

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.

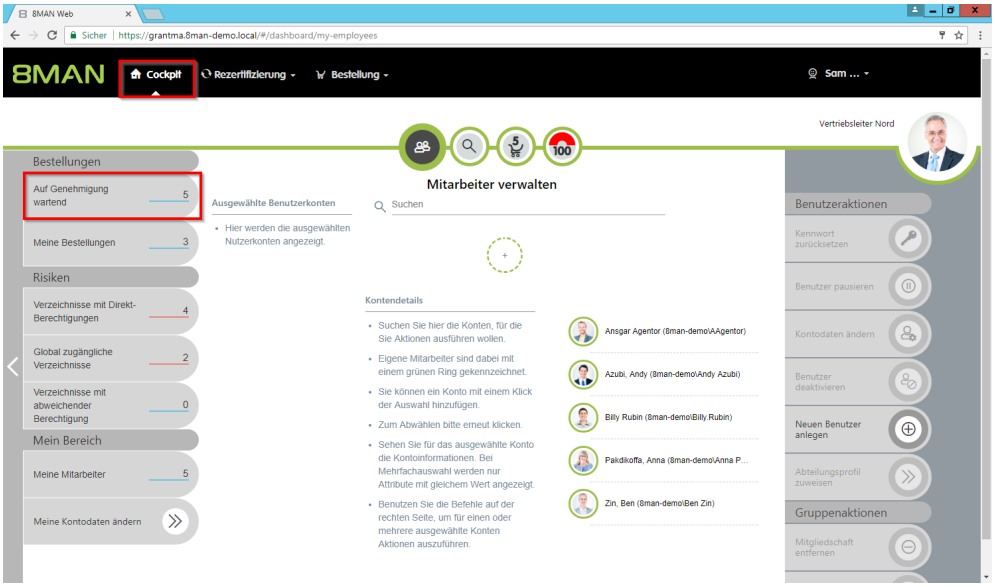
Weiterführende Services

Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

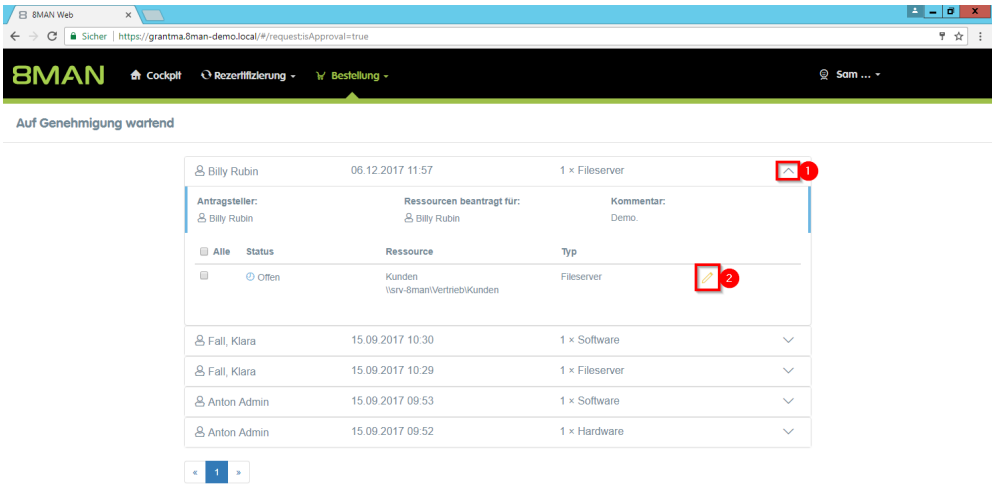


Melden Sie sich als Genehmiger an.

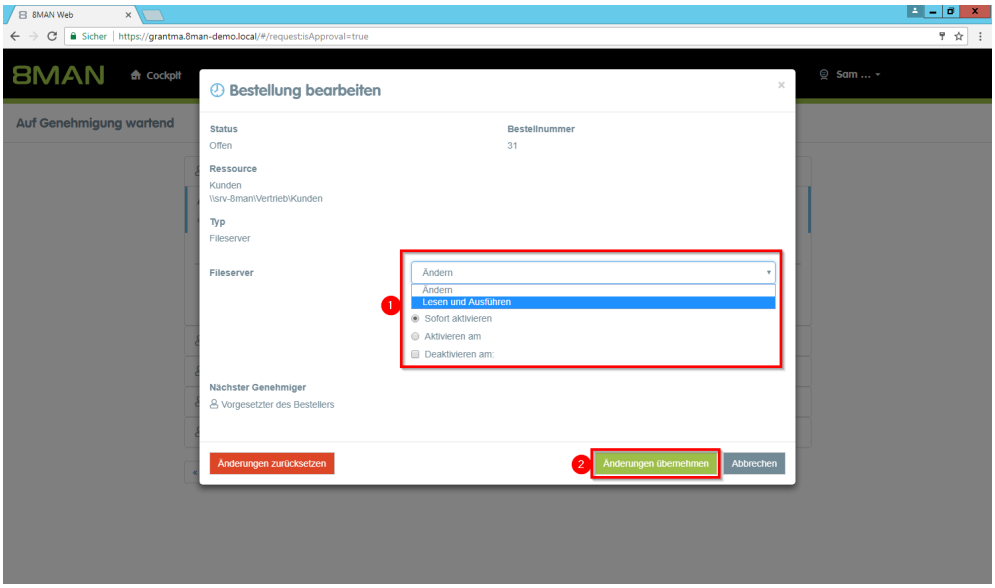


Klicken Sie auf "Auf Genehmigung wartend". In dem gezeigten Beispiel warten 5 Anträge auf Genehmigung.

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

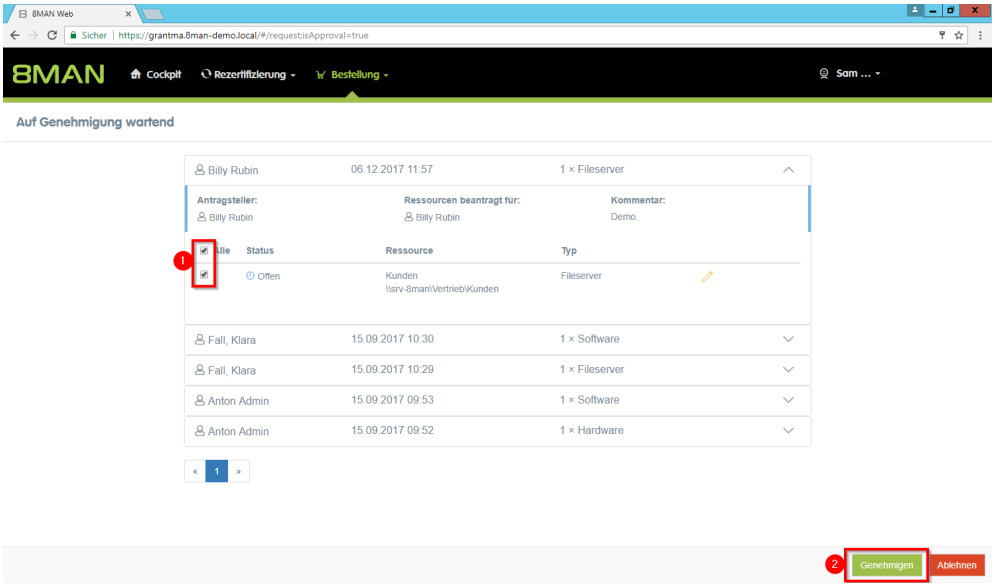


1. *Klappen Sie eine Bestellung auf, um die Positionen sehen zu können.*
2. *Lassen Sie sich Details zu den einzelnen Positionen einblenden.*
   Je nach Konfiguration sehen Sie ein Stift- oder ein Informationssysmbol.
   Stift: Sie können die Bestellung anpassen.
   Info: Sie sehen die Details.
   Klicken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

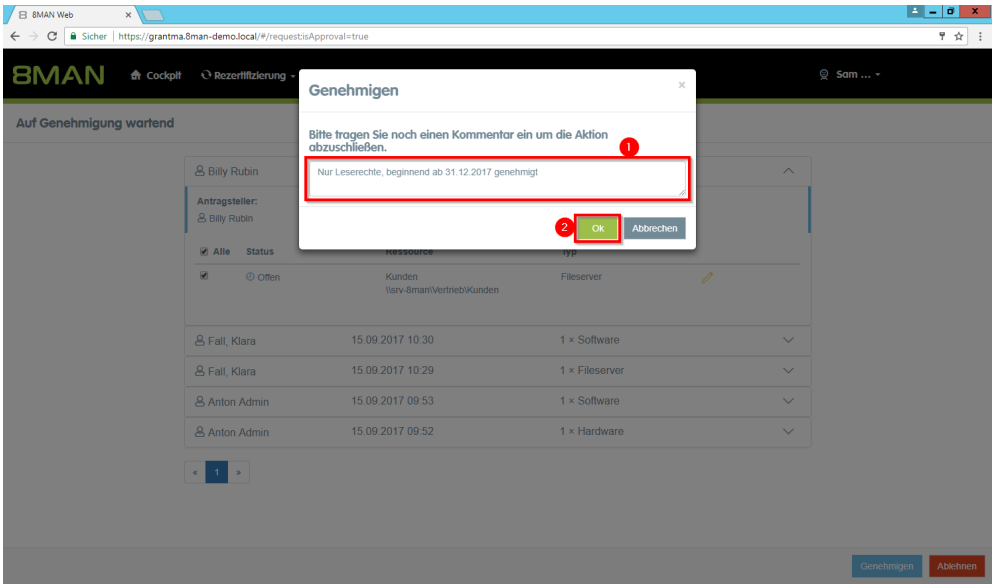


Sie können die Bestellanfrage bearbeiten.

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.

3.1.5.2 Risiken

Im Bereich Risiken sehen Sie die drei am höchsten bewerteten Risikokriterien aus dem Risk Assessment Dashboard.

Die Risikokriterien sind:

seit Release 9

Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check)

bereits seit Release 8 vorhanden

Inaktive Konten
Rekursive Gruppen
Benutzer mit nie ablaufenden Kennwörtern
Global zugängliche Verzeichnisse
Unaufgelöste SIDs
Direktberechtigungen
Verzeichnisse mit abweichenden Berechtigungen

3.1.5.2.1 Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check)

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.

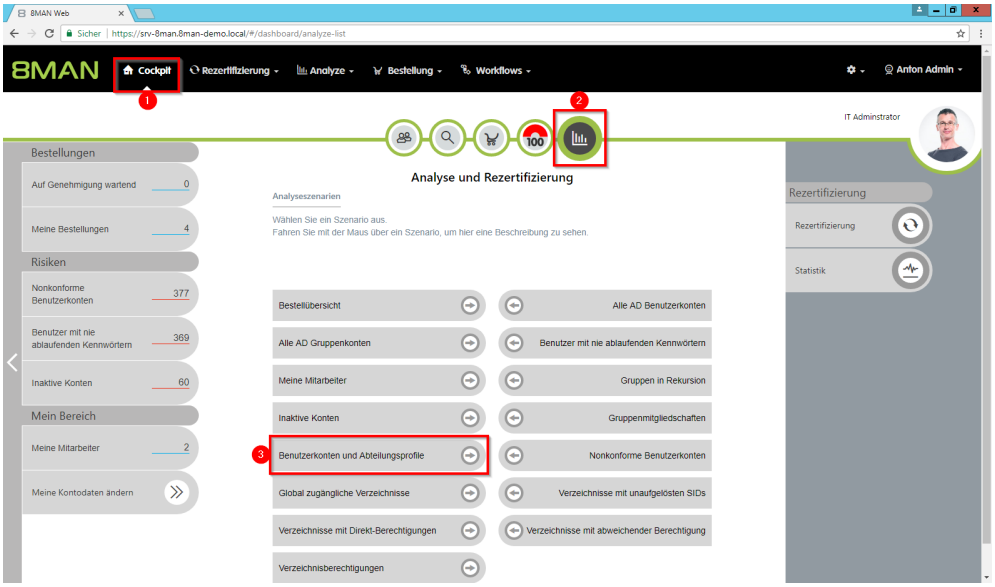
Erhält der Mitarbeiter weitere Berechtigungen, die vom Standard abweichen, zeigt ein Compliance-Monitor dem Vorgesetzten die abweichenden Rechte. In Form von Bulk-Operationen, kann der Abteilungsleiter die Nutzerkonten entsprechend der Profile in seiner Abteilung harmonisieren.

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

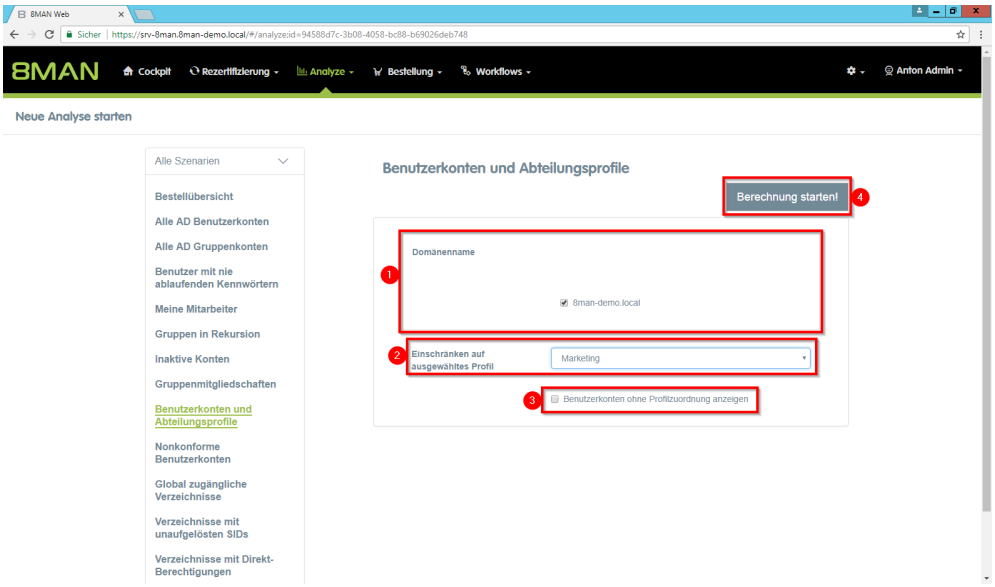
Weiterführende Services

Ein neues Abteilungsprofil erstellen (Administrator)
Benutzern ein Abteilungsprofil zuweisen

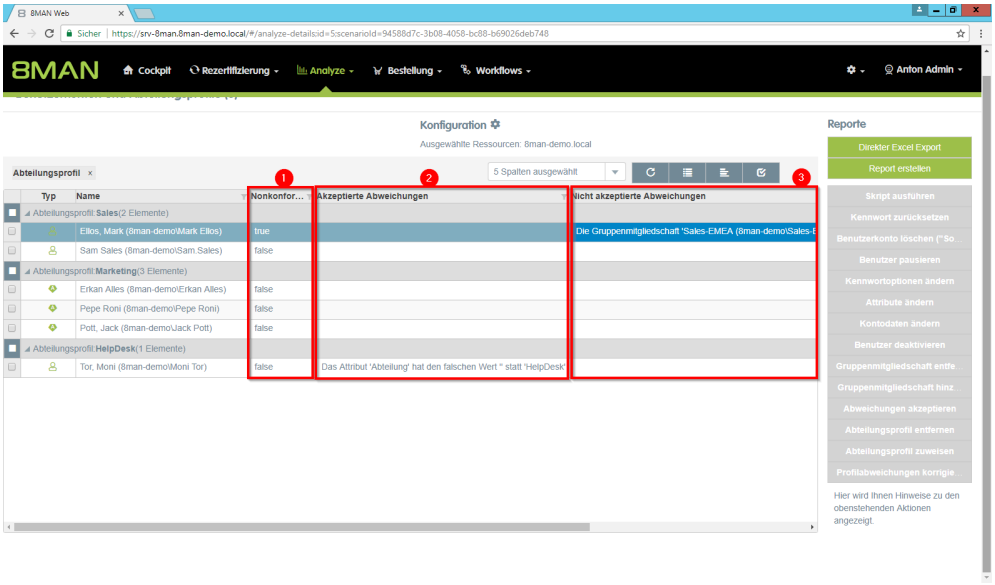
Der Prozess in einzelnen Schritten



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.*

3.1.5.3 Mein Bereich

3.1.5.3.1 Die eigenen Kontodaten ändern (Cockpit)

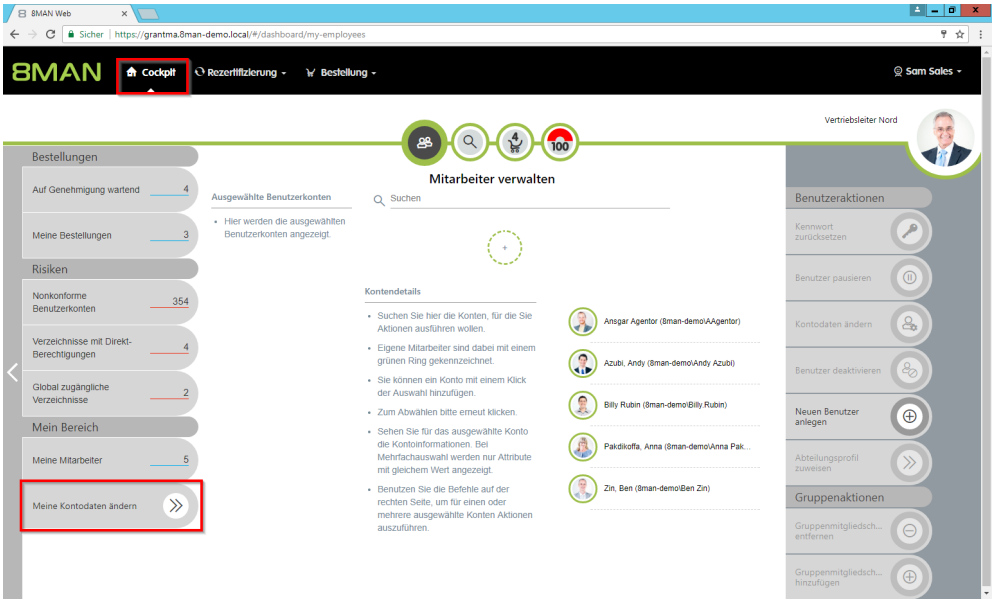
Hintergrund / Mehrwert

Mit 8MAN können Sie schnell und komfortabel die eigenen Kontoinformationen ändern. Die Aktionen werden für die Revision dokumentiert.

Weiterführende Services

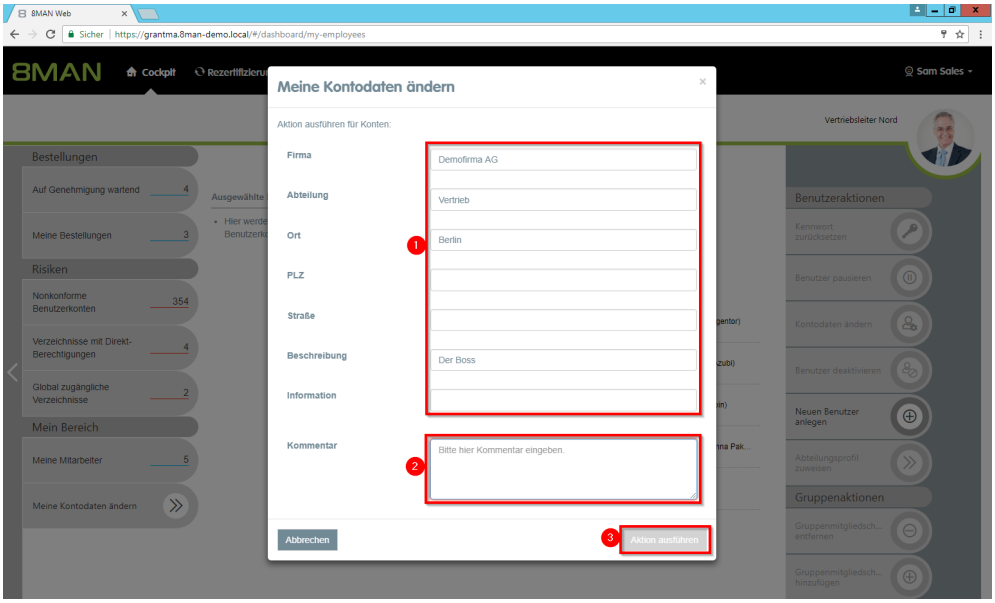
Übersicht aller Cockpit-Services

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".*

3.1.5.3.2 Meine Mitarbeiter verwalten (Cockpit)

Hintergrund / Mehrwert

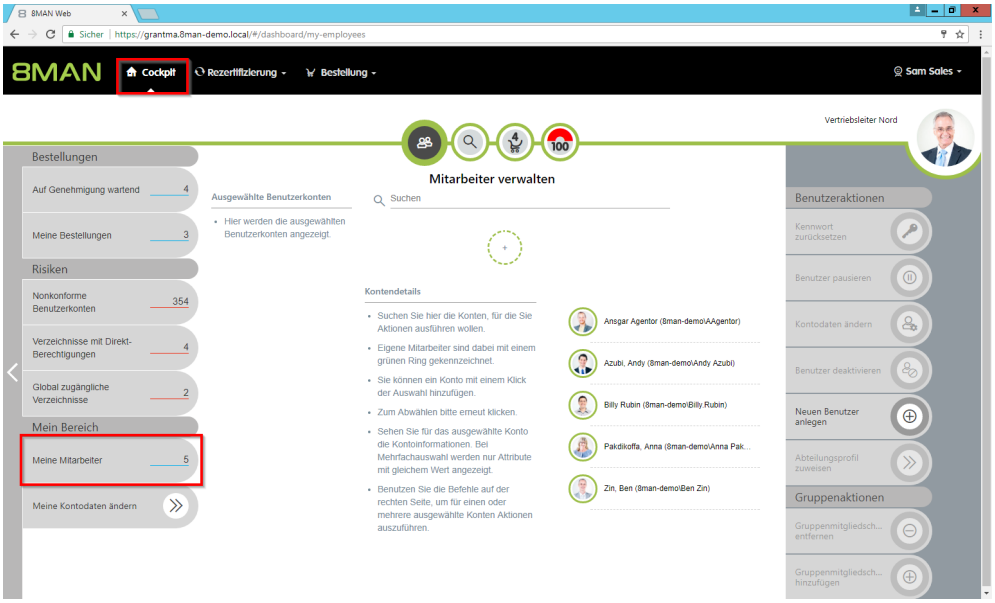
Mit 8MAN können Sie schnell und komfortabel die Ihnen zugeordneten Mitarbeiter verwalten. Aktionen werden für die Revision dokumentiert.

Mitarbeiter sind Benutzer, bei denen Sie als "Vorgesetzter" im Active Directory eingetragen sind. Fragen Sie dazu Ihren Administrator.

Weiterführende Services

Übersicht aller Cockpit-Services

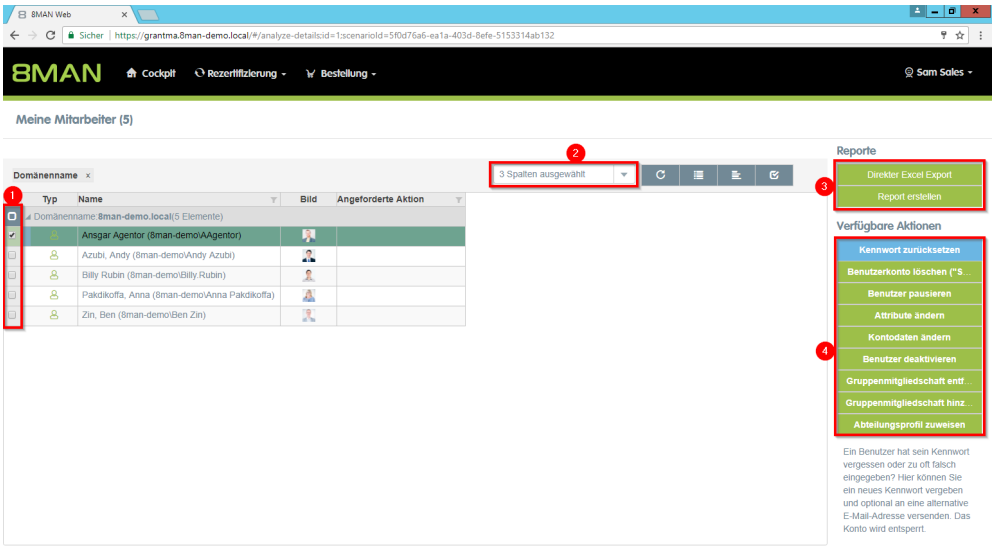
Der Prozess in einzelnen Schritten



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.*

3.1.5.4 Benutzeraktionen

3.1.5.4.1 Kennwörter von Benutzern zurücksetzen (Cockpit)

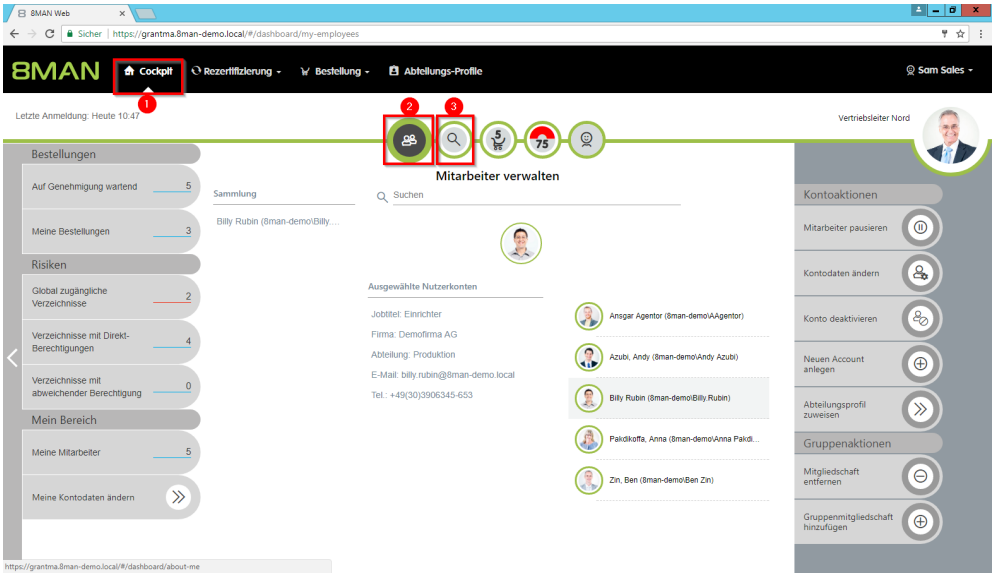
Hintergrund / Mehrwert

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.

Weiterführende Services

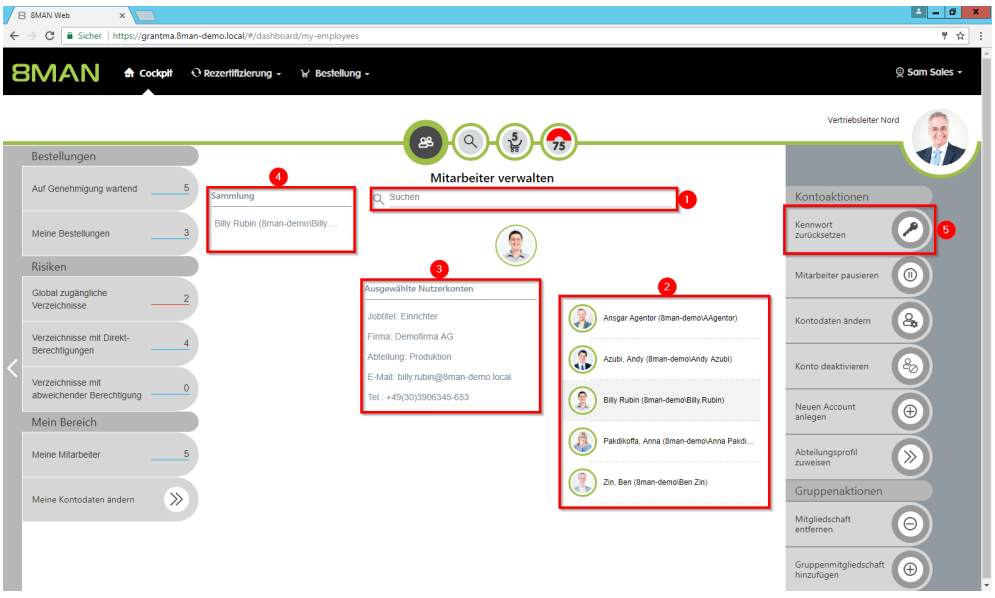
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

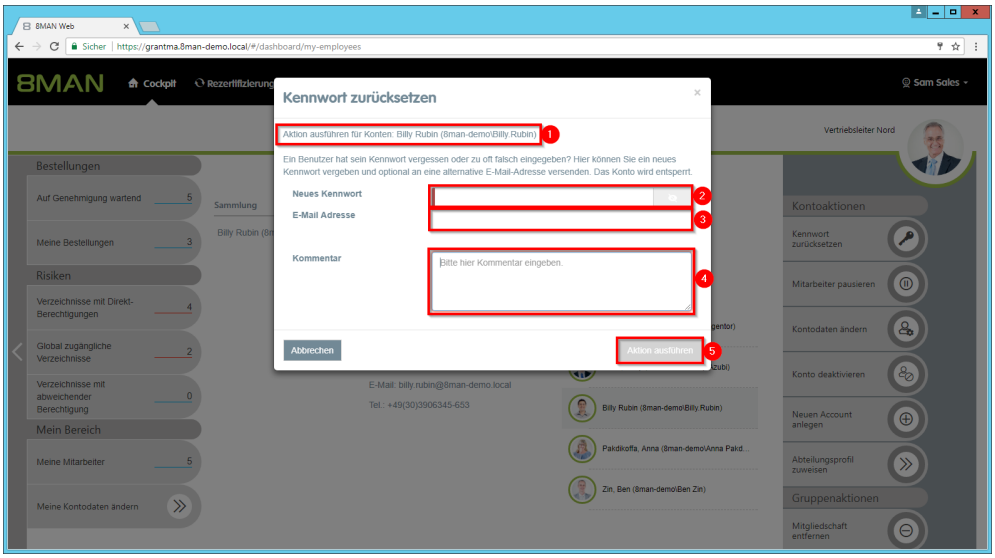


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter werden Ihnen von einem Administrator über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Benutzer verwalten. Benutzer werden Ihnen von einem Administrator über die 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".*

3.1.5.4.2 Kontodaten von Benutzern ändern (Cockpit)

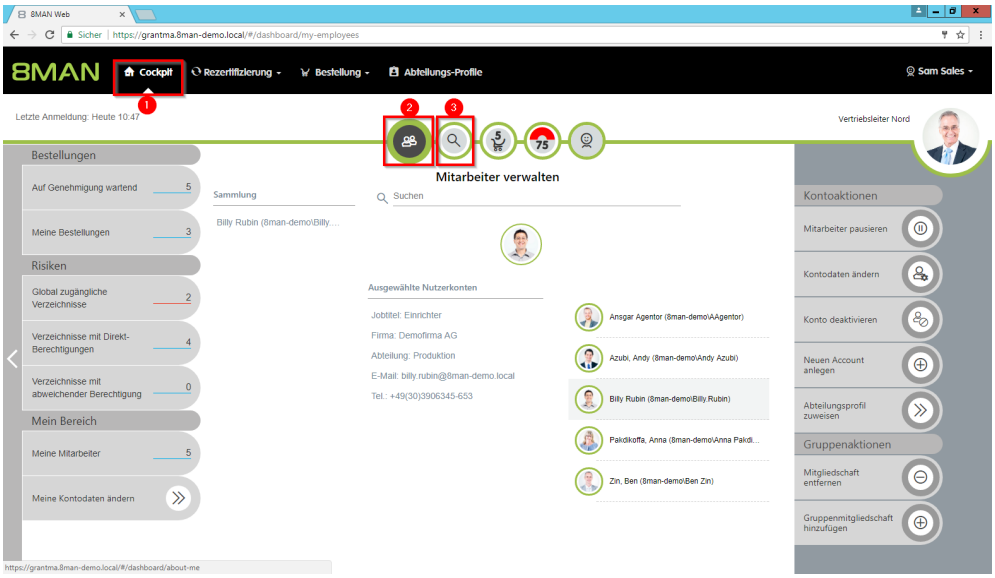
Hintergrund / Mehrwert

Mit 8MAN können Sie schnell und komfortabel Kontoinformationen von Benutzern ändern, auch von mehreren in einem Arbeitsgang. Die Aktionen werden revisionssicher dokumentiert.

Weiterführende Services

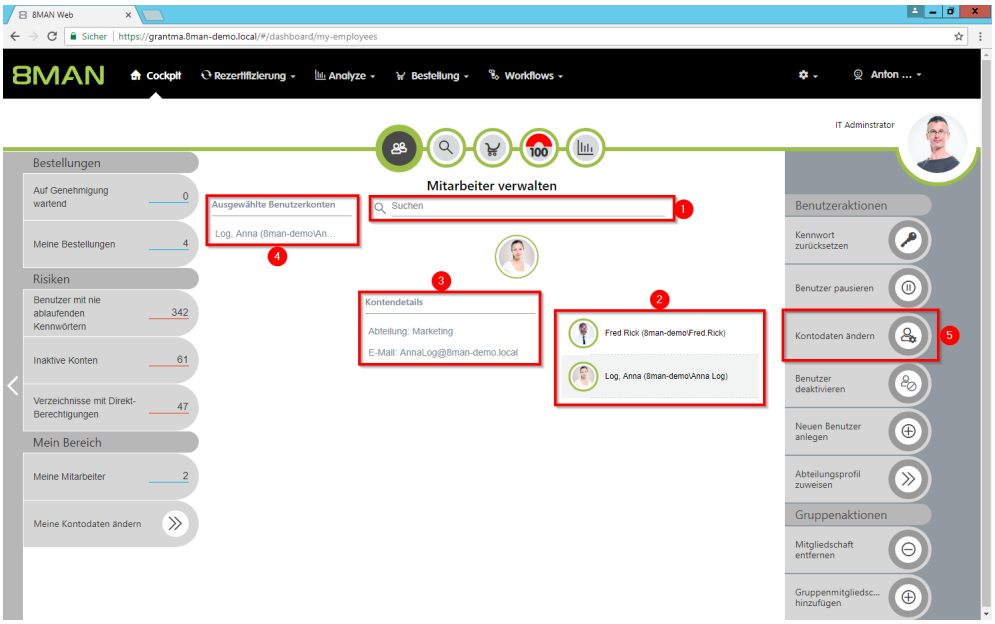
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

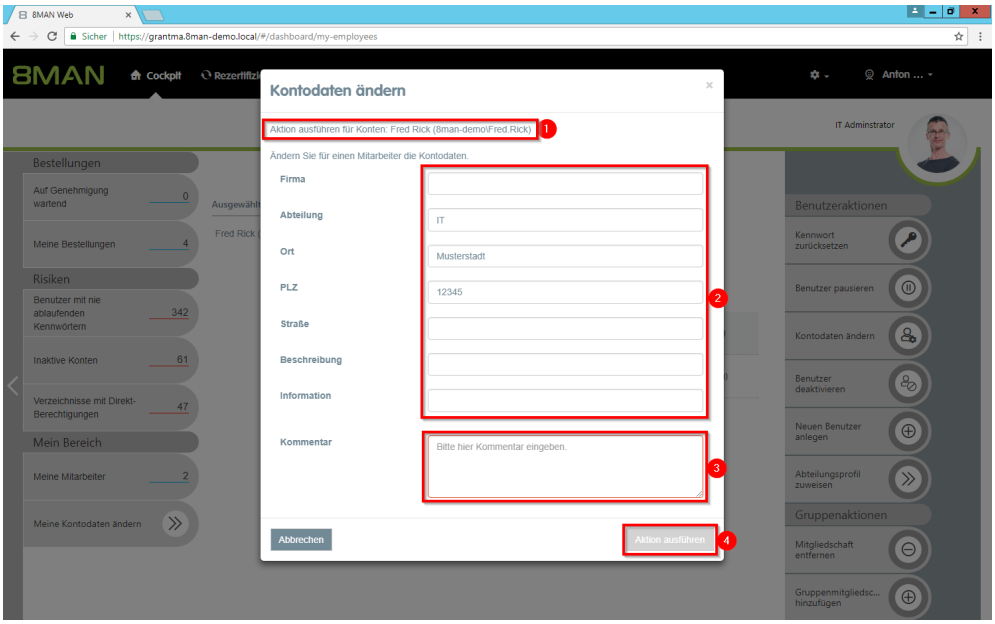


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

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".*

3.1.5.4.3 Benutzer deaktivieren (Cockpit)

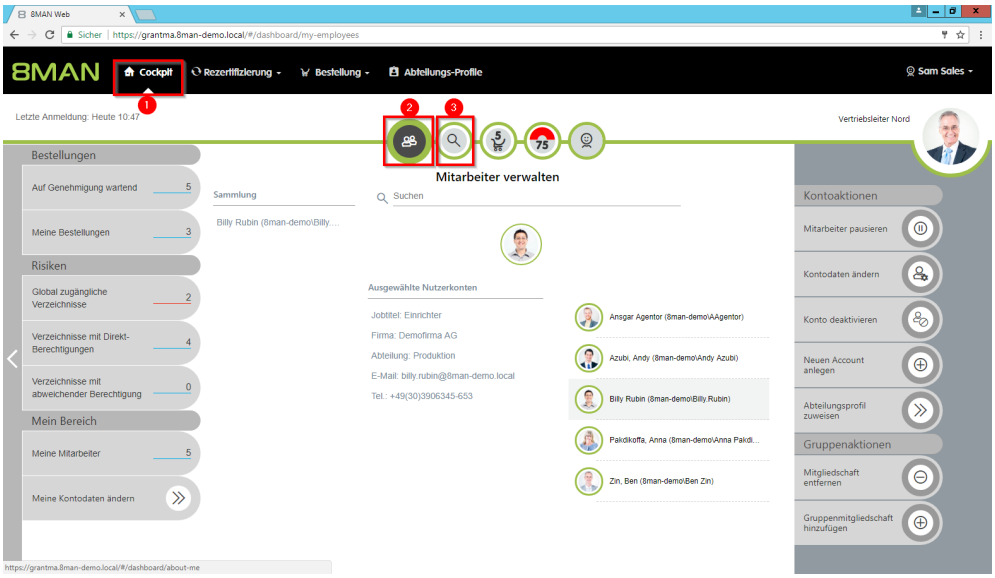
Hintergrund / Mehrwert

Deaktivieren Sie mit 8MAN einen Benutzer in wenigen Schritten. Deaktivieren Sie bei einer Entlassung frühzeitig ein Nutzerkonto.

Weiterführende Services

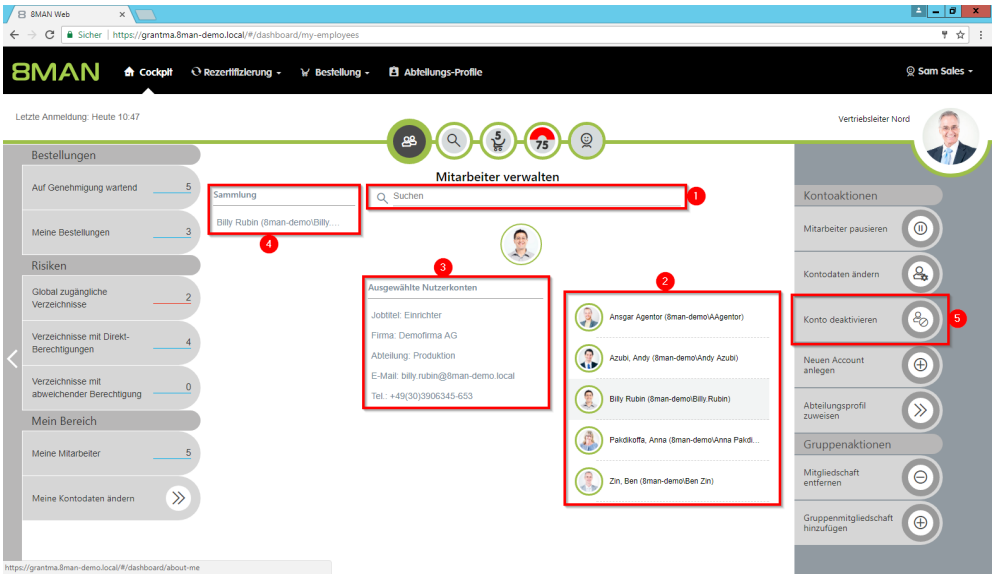
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

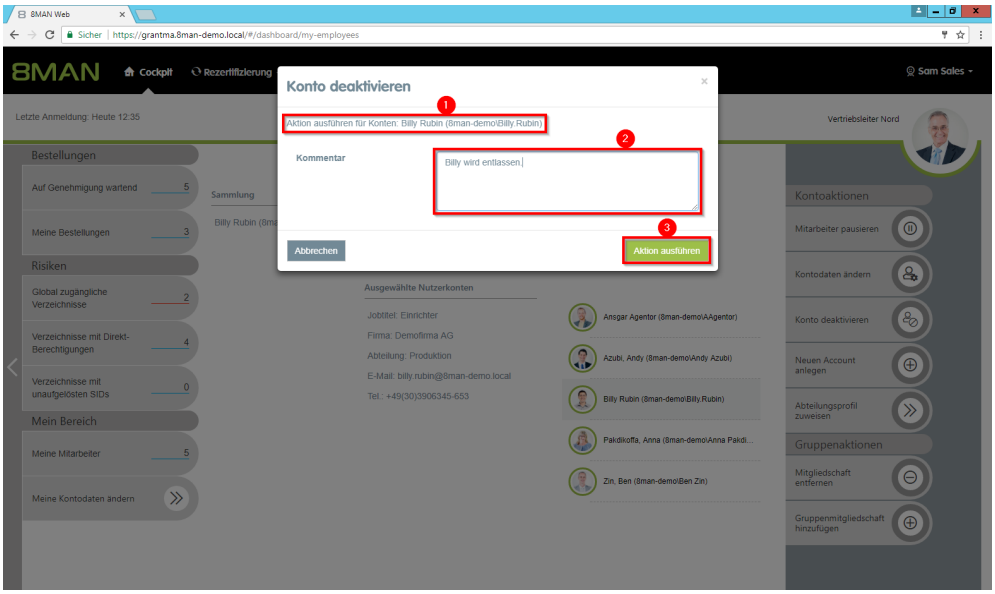


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

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".*

3.1.5.4.4 Benutzer pausieren (Cockpit)

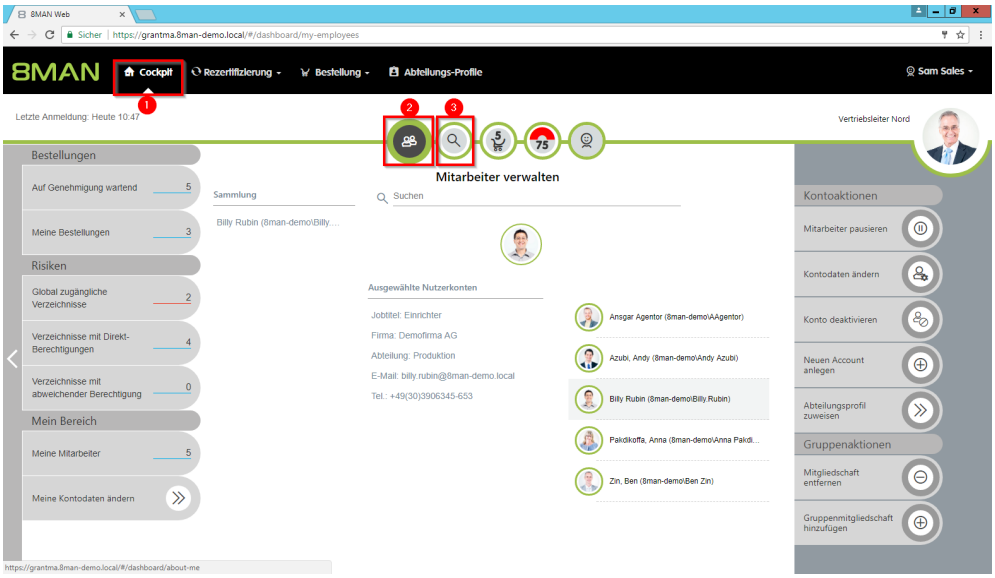
Hintergrund / Mehrwert

Pausieren Sie einen Mitarbeiter in wenigen einfachen und schnellen Schritten, z. B. bei Elternzeit.

Weiterführende Services

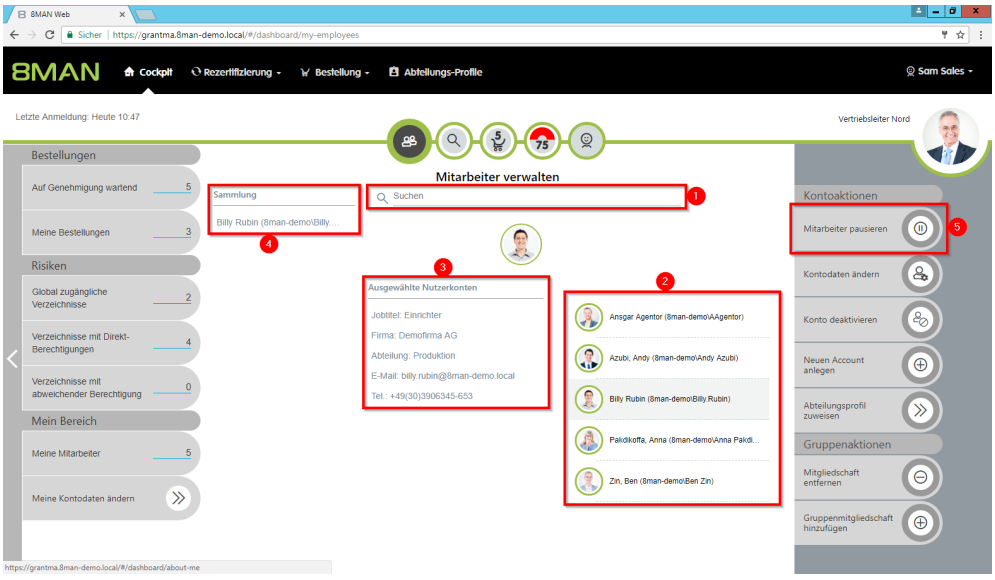
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

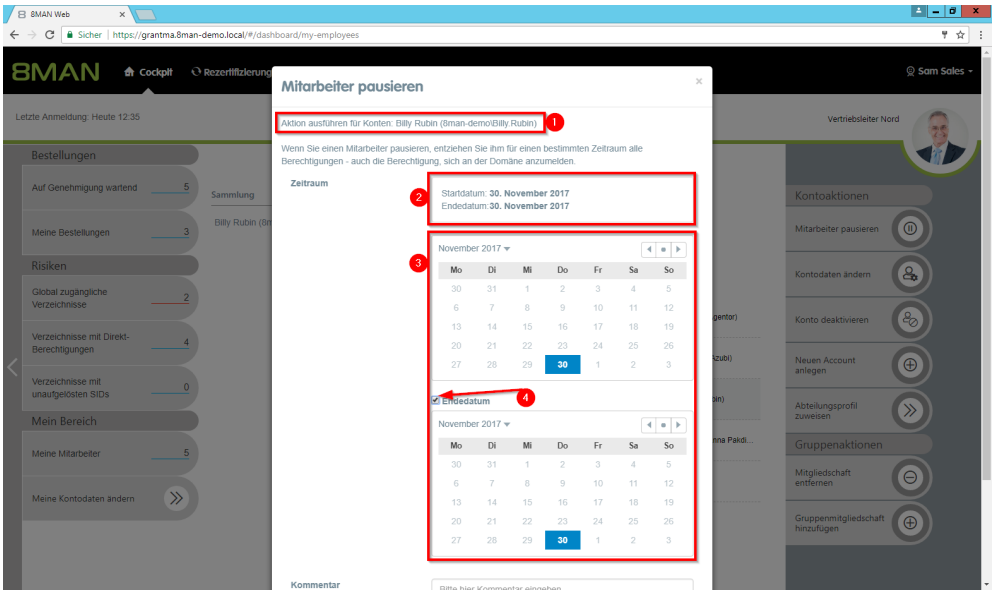


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

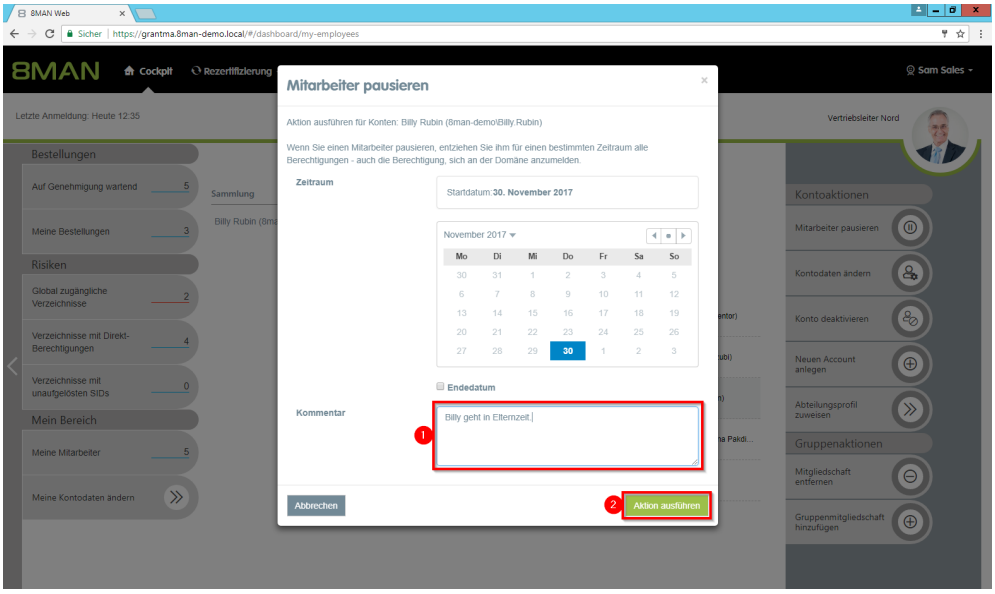
Der Umfang der verfügbaren Services (Schaltflächen) variiert nach Rolle (Login), Risikolage und Konfiguration.



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".*

3.1.5.4.5 Einen neuen Benutzer anlegen (Cockpit)

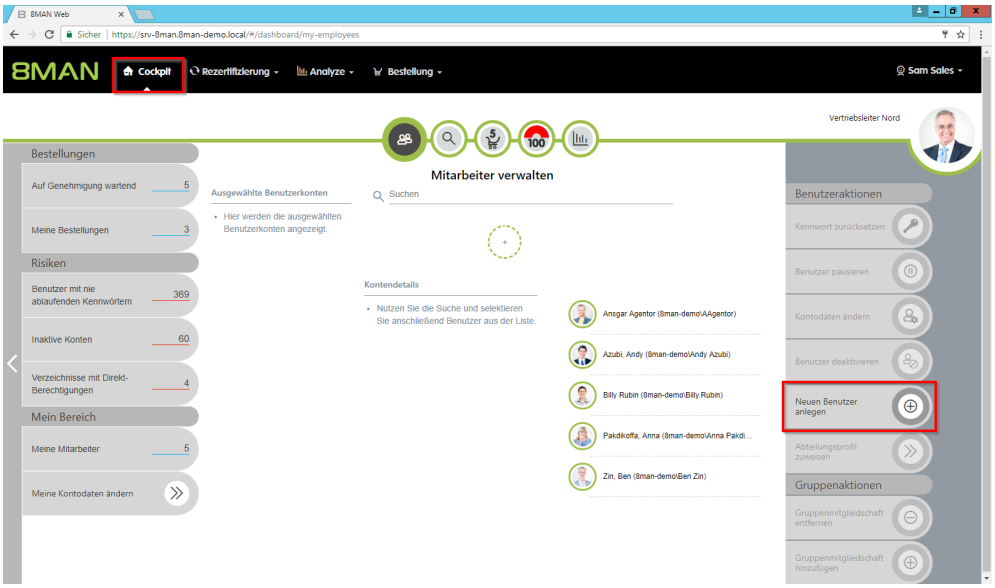
Hintergrund / Mehrwert

Legen Sie im Webclient einen neuen Benutzer an. Die Neuanlage basiert auf von Administratoren vordefinierten Templates und erfolgt deshalb effizient und standardisiert.

Weiterführende Services

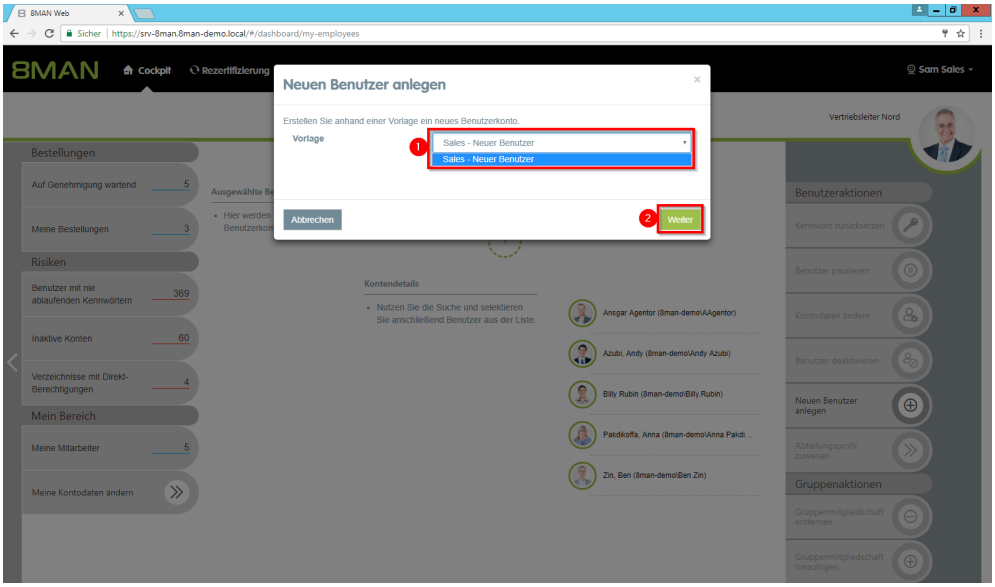
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

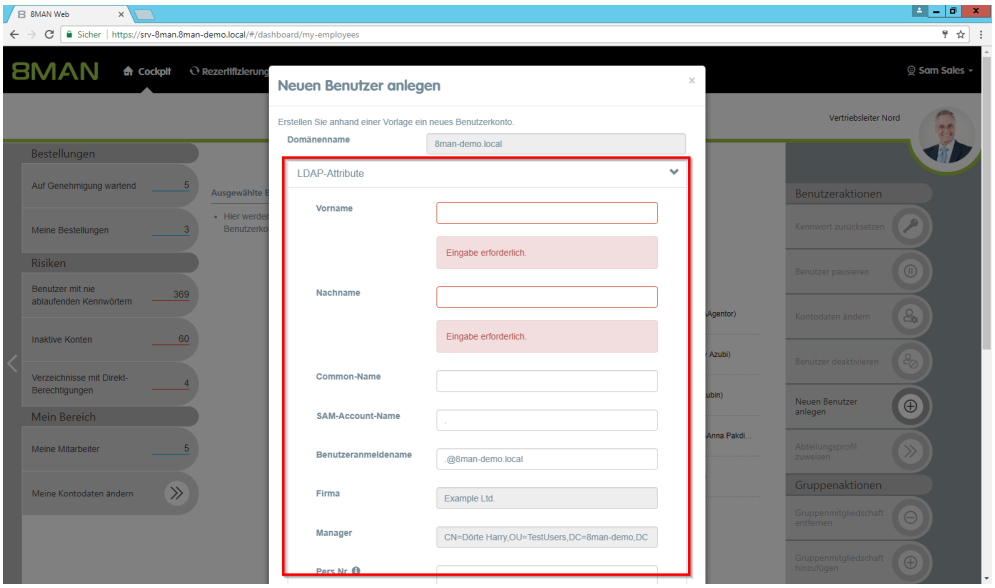


1. *Klicken Sie im Cockpit auf "Neuen Benutzer anlegen".*

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

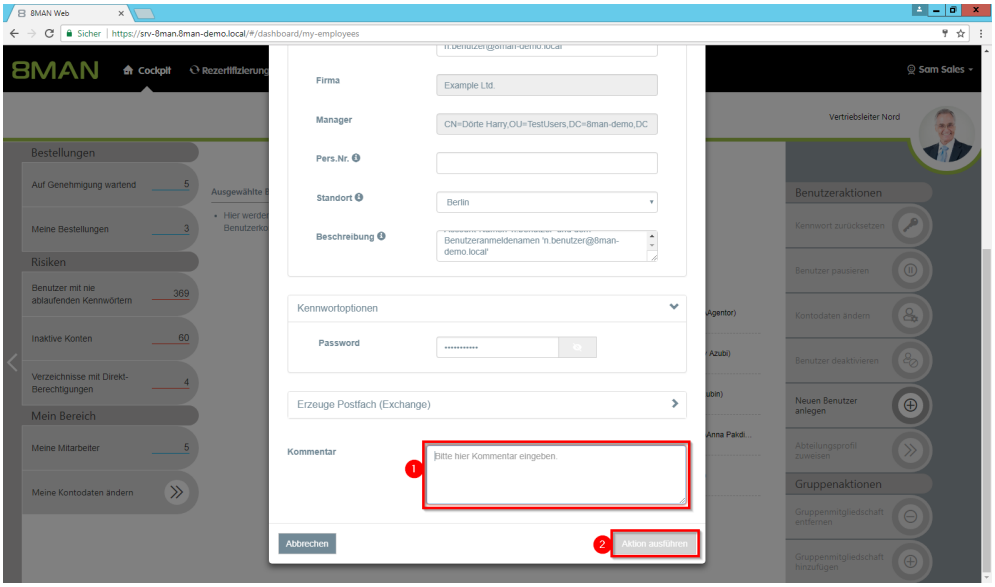


1. *Wählen Sie eine Vorlage aus.*
2. *Klicken Sie auf "Weiter".*



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".*

3.1.5.4.6 Benutzern ein Abteilungsprofil zuweisen (Cockpit)

Hintergrund / Mehrwert

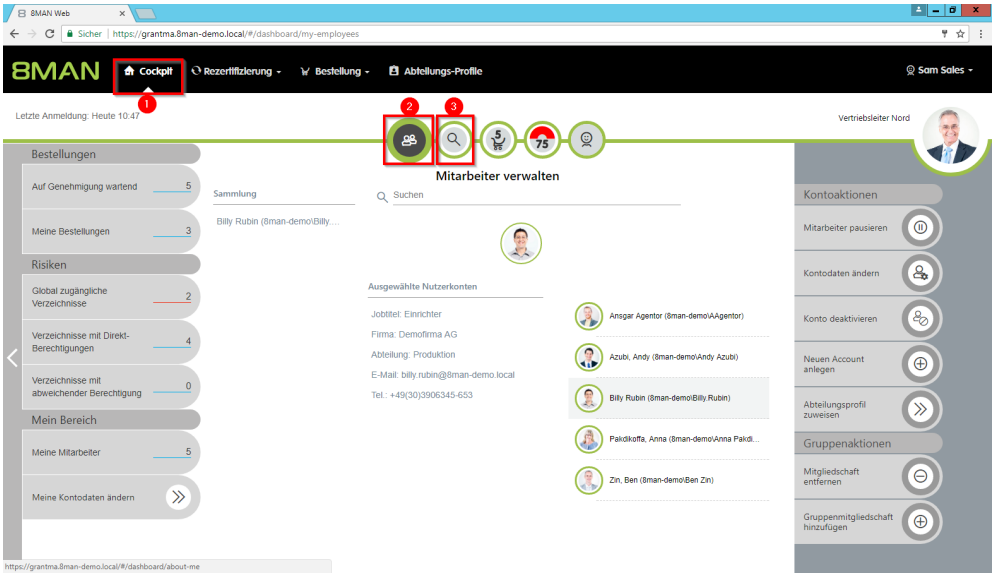
Mit einem Abteilungsprofil weisen Sie einem Benutzer einen Basissatz an Berechtigungen zu. Wechselt der Mitarbeiter die Abteilung, kann der Vorgesetzte einfach ein Abteilungsprofil anwenden. Die alten Berechtigungen können dabei gleich entfernt werden.

Weiterführende Services

Ein neues Abteilungsprofil erstellen

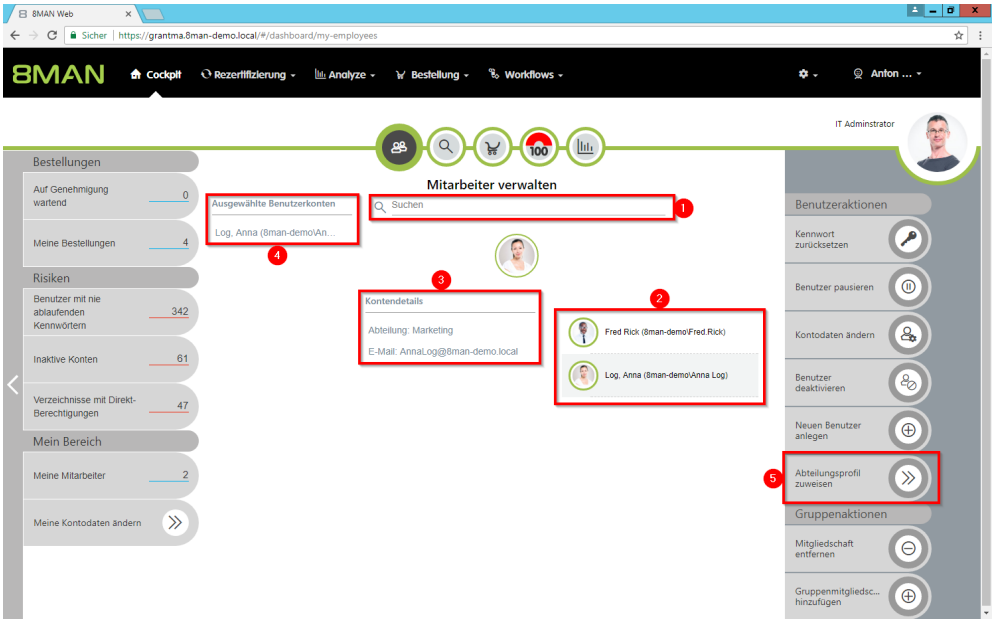
Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check)

Der Prozess in einzelnen Schritten

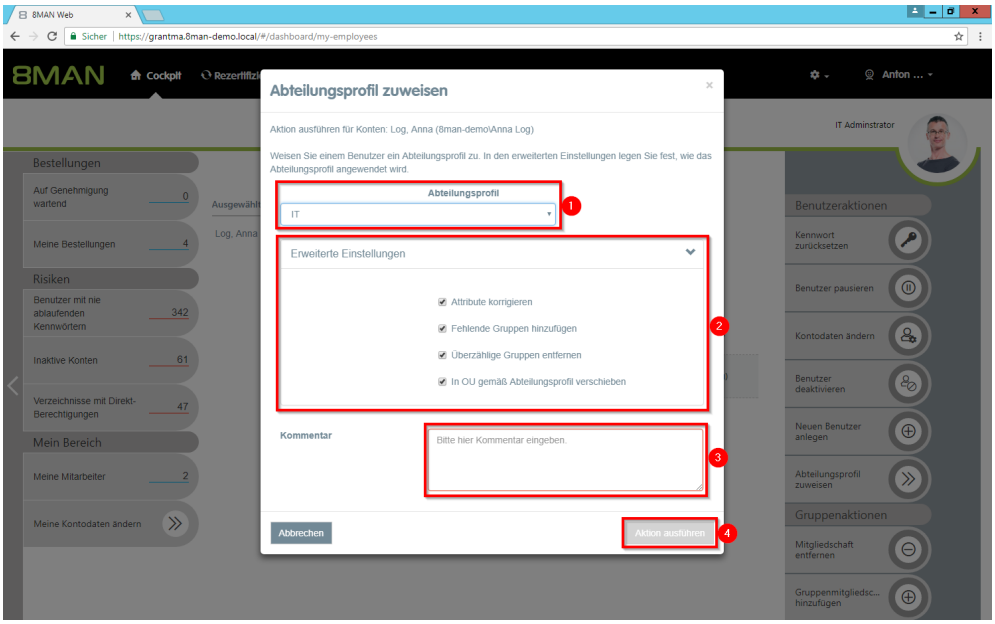


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

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".*

3.1.5.5 Gruppenaktionen

3.1.5.5.1 Gruppenmitgliedschaften entfernen (Cockpit)

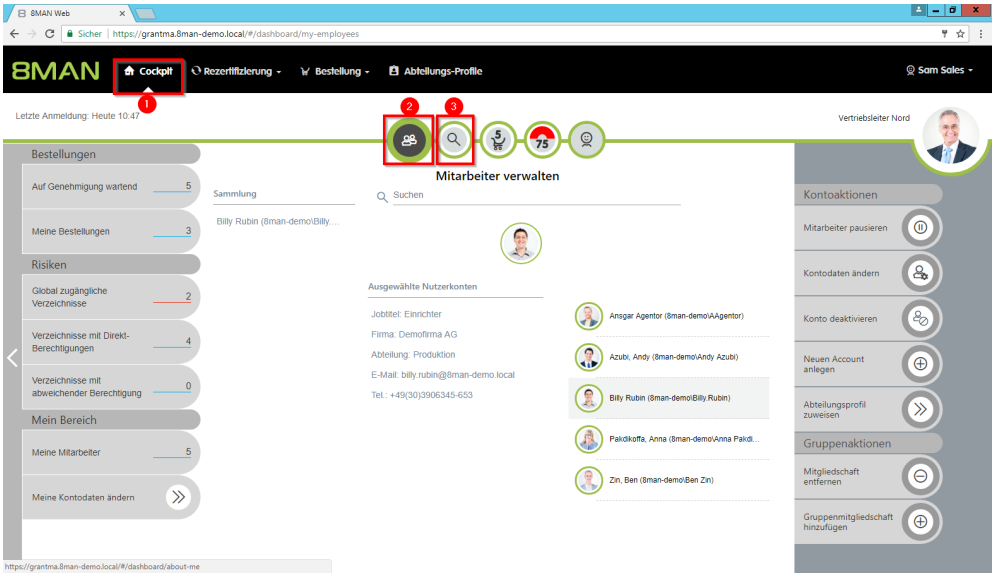
Hintergrund / Mehrwert

Überberechtigungen entstehen häufig durch Gruppenmitgliedschaften. Im Cockpit können Sie schnell Gruppenmitgliedschaften entfernen.

Weiterführende Services

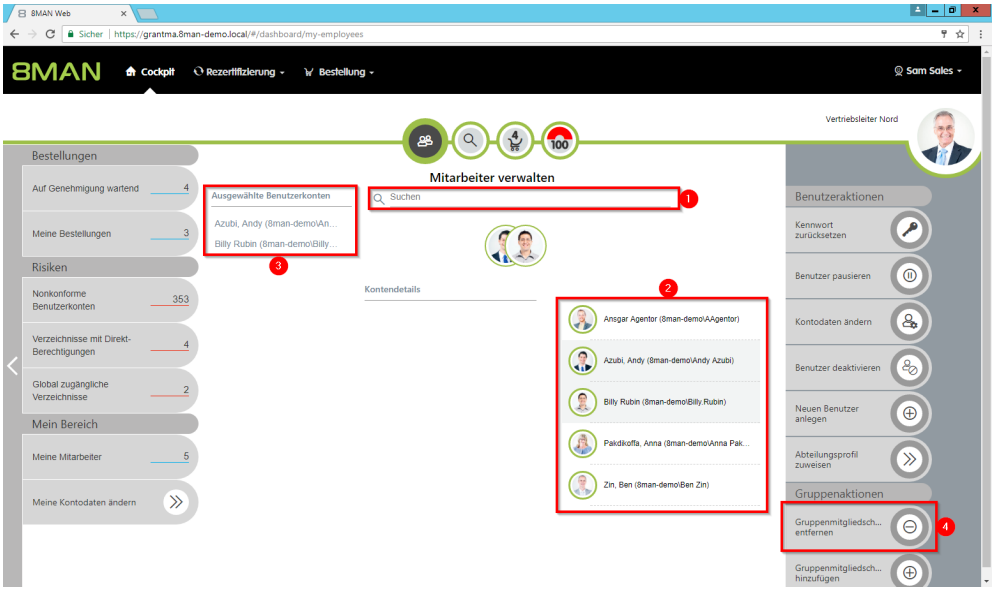
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

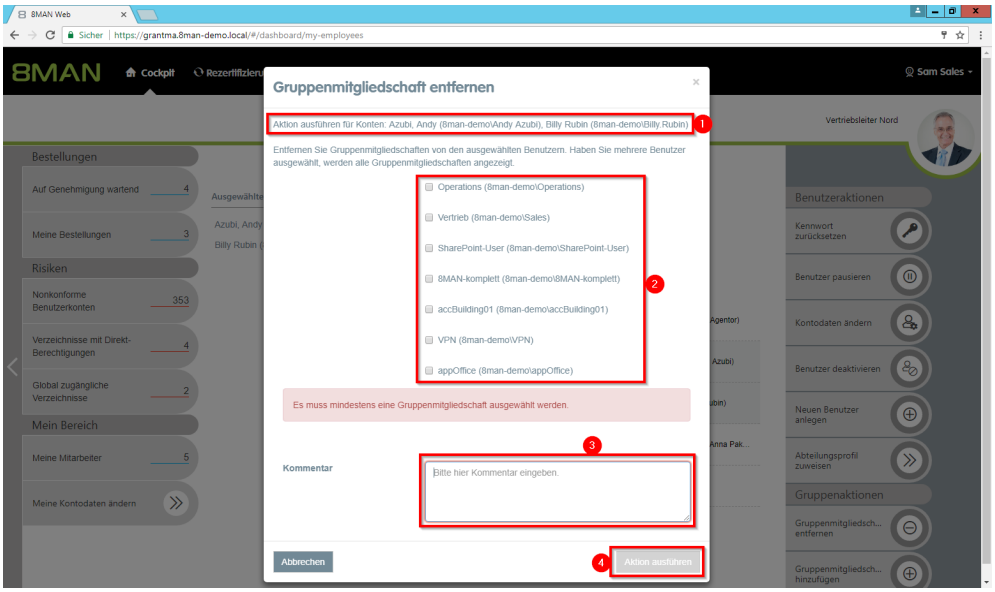


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

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".*

3.1.5.5.2 Gruppenmitgliedschaften hinzufügen (Cockpit)

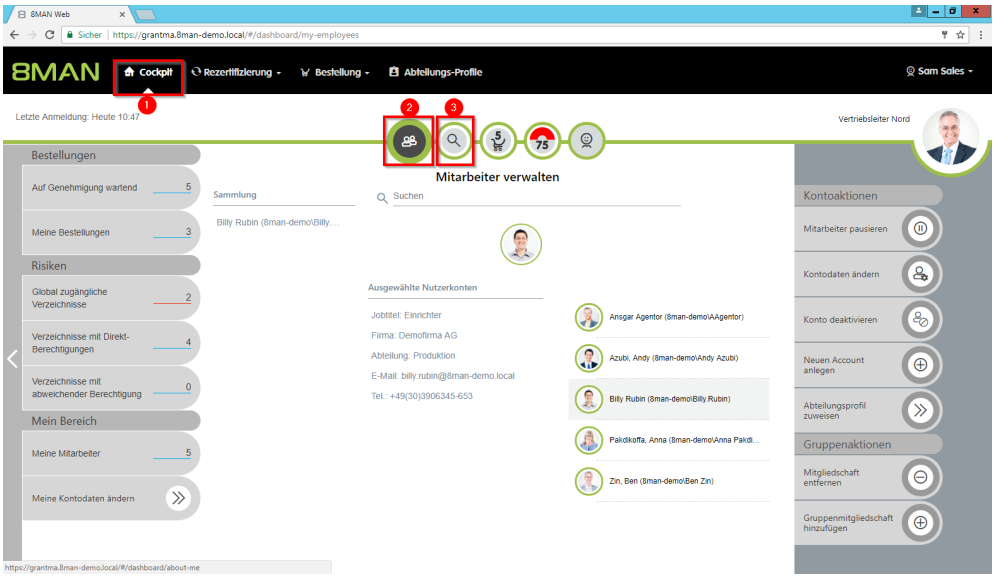
Hintergrund / Mehrwert

Stellt z. B. ein Manager fest, dass seinem Mitarbeiter eine Gruppenmitgliedschaft fehlt, kann er diese in wenigen einfachen Schritten hinzufügen.

Weiterführende Services

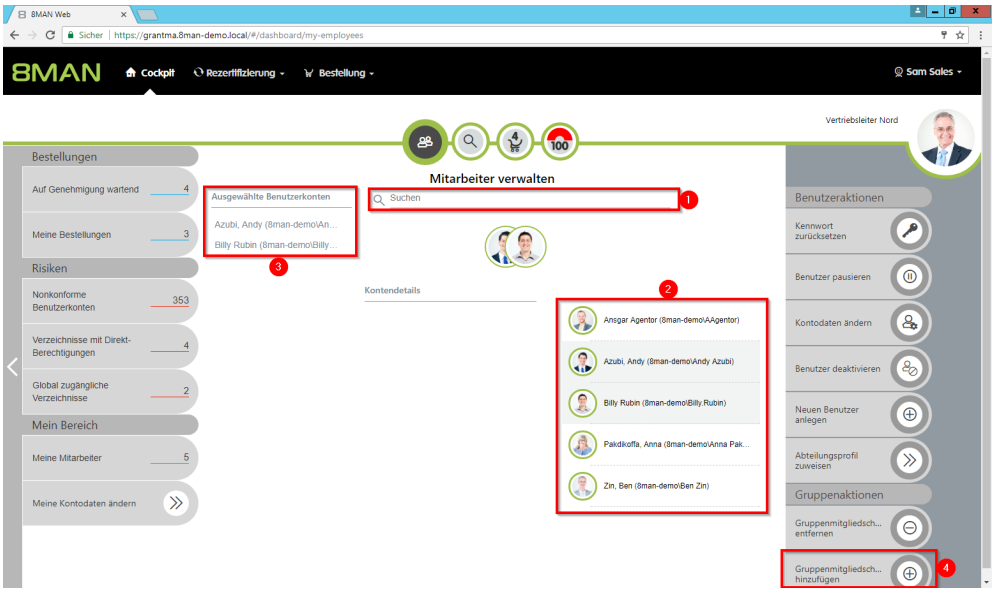
Übersicht aller Cockpit-Services

Der Prozess in einzelnen Schritten

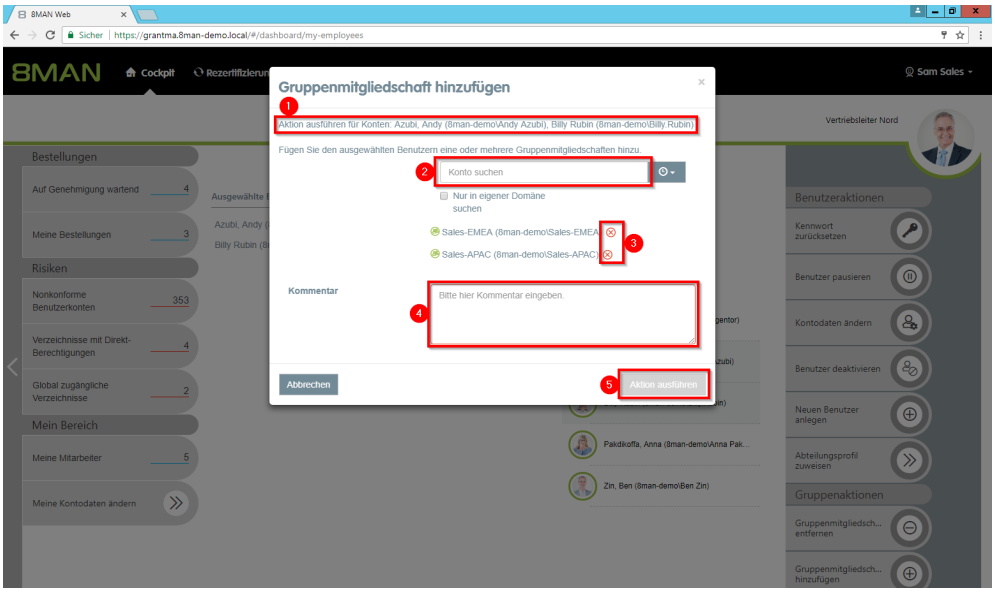


1. *Wählen Sie Cockpit.*
2. *Wählen Sie "Mitarbeiter verwalten". Mitarbeiter sind Ihnen über das Active Directory Attribut "Vorgesetzter" zugeordnet. Siehe Attribute ändern (Webclient).*
3. *Wählen Sie Konten verwalten. Konten werden Ihnen über die Data-Owner-Konfiguration zugeordnet.*

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".*

4 Security Monitoring

4.1 8MATE FS Logga: Alarme für Fileserver

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.

Folgende mögliche Sicherheitsvorfälle indiziert 8MAN:

- Datendiebstahl: Ein Nutzerkonto liest in einem kurzen Zeitraum ungewöhnlich viele Dateien ein („File read“)
- Datenlöschungen: Ein Nutzerkonto löscht in einem kurzen Zeitraum sehr viele Dateien („File delete“)
- Ransomware Attacke: Von einem Nutzerkonto geht die Kombination aus Dateierstellung und Löschung aus („File create“ & „File delete“)

Folgende Events konfigurieren Sie als Auslöser für Alerts:

- Datei gelesen
- Datei geschrieben
- Verzeichnis erstellt
- Datei erstellt
- Verzeichnis verschoben/umbenannt
- Datei verschoben/umbenannt
- Verzeichnis gelöscht
- Datei gelöscht
- Berechtigung geändert (ACL changed)

Definieren Sie Schwellenwerte anhand der Häufigkeit der Events als auch der Zeitabstände. Serviceaccounts, Administratorenkonten und spezielle Verzeichnisse nehmen Sie über eine Blacklist aus der Alarmfunktion heraus.

Gezielt sicherheitskritische Verzeichnisse überwachen

Darüber hinaus lassen sich auch verzeichnisspezifisch Alarme definieren. Sollte ein unbekanntes Nutzerkonto Zugriff auf ein sicherheitsrelevantes Verzeichnis erhalten, sendet 8MAN einen Alarm an die Datenverantwortlichen.

Skripte nach einem Alarm automatisch ausführen

Wird ein Fileserver oder Active Directory Alarm ausgelöst, kann 8MAN anschließend ein Skript ausführen. Dies ist z.B. im folgenden Szenario relevant:

Ein Nutzerkonto wird der überwachten Administratorengruppe hinzugefügt. Ein Alert wird sofort ausgelöst und das verknüpfte Skript entfernt das Nutzerkonto sofort wieder aus der Gruppe. Damit ist die Administratorengruppe dauerhaft vor Manipulation geschützt.

Alarme priorisieren

Ab Version 9 priorisieren Sie die Alarme entsprechend der Kategorien in der Windows Ereignisanzeige. Darüber hinaus werden kategorisierte Alert-E-Mails versendet.

Services

Alarme für Fileserververzeichnisse aktivieren
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

4.1.1 Alarme für Fileserververzeichnisse aktivieren

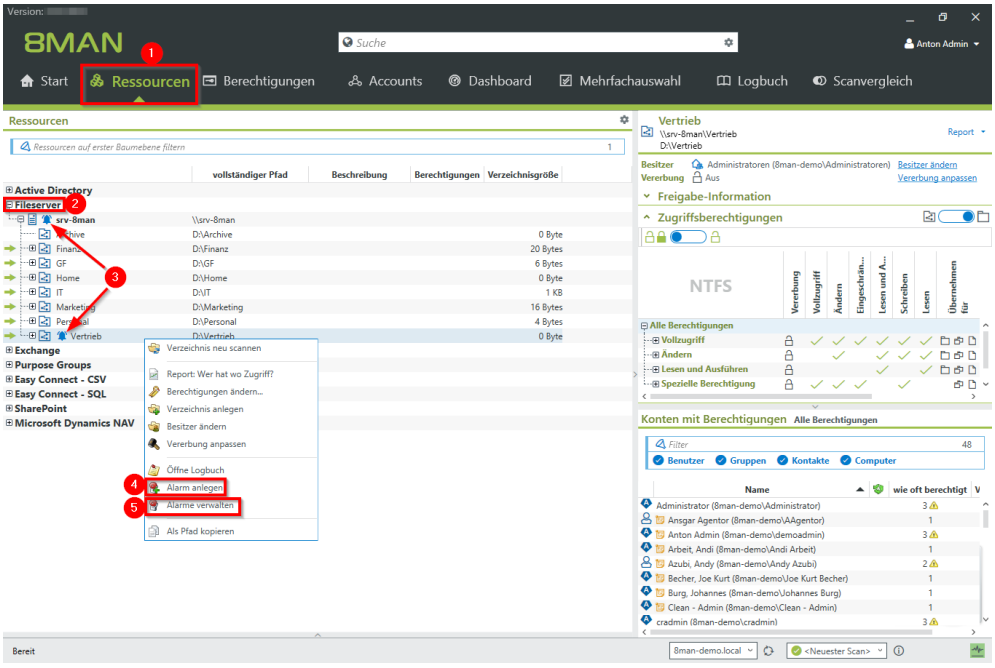
Hintergrund / Mehrwert

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.

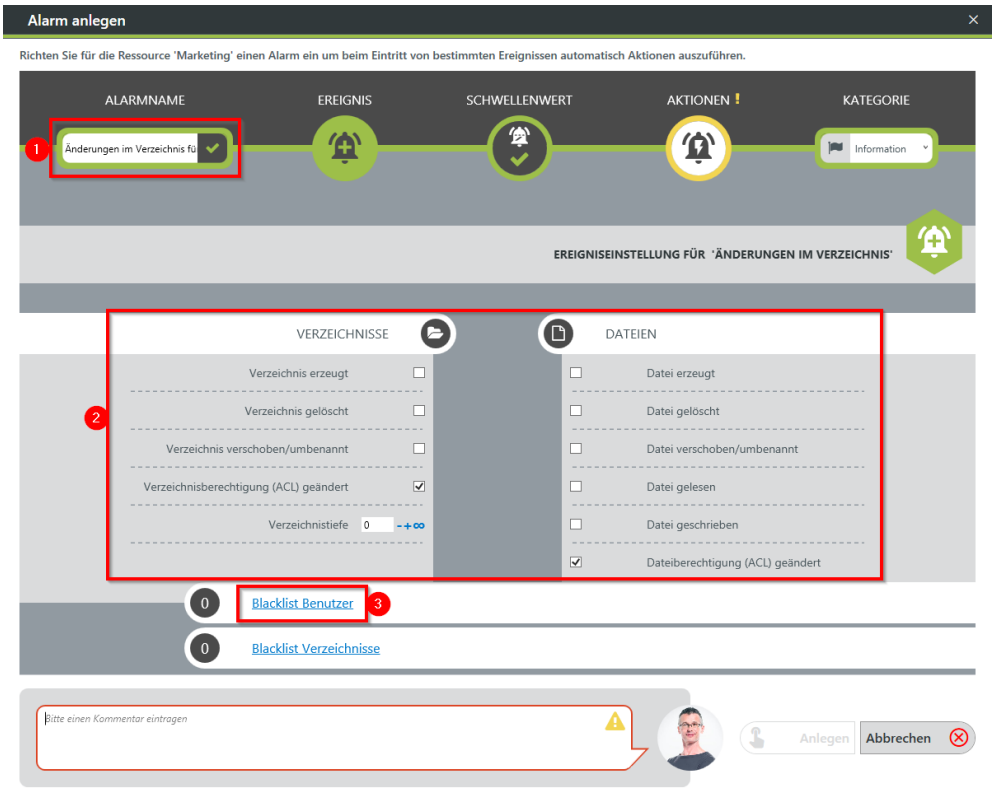
Weiterführende Services

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

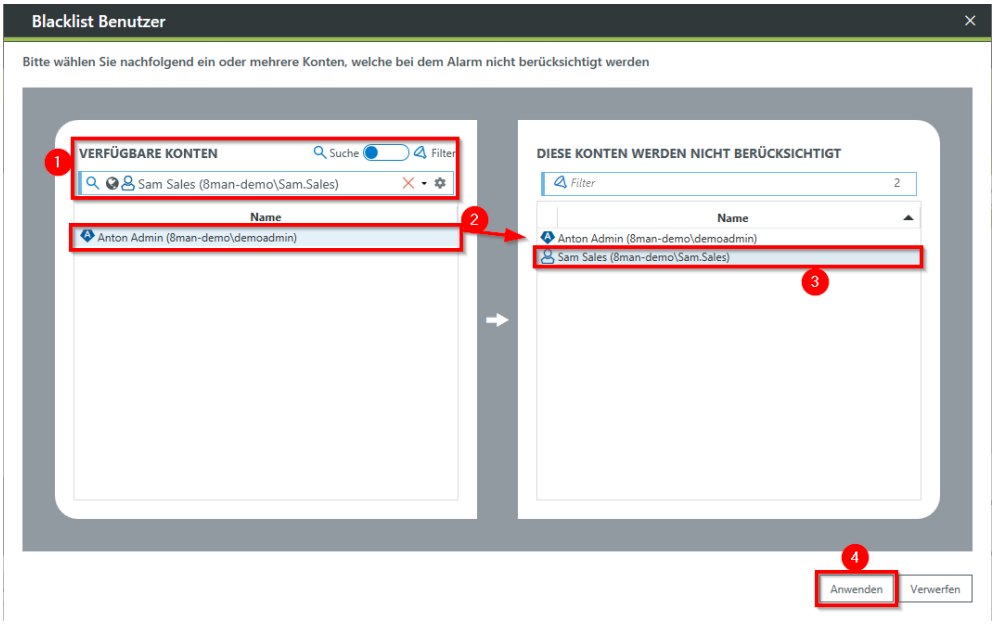
Der Prozess in einzelnen Schritten



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".*



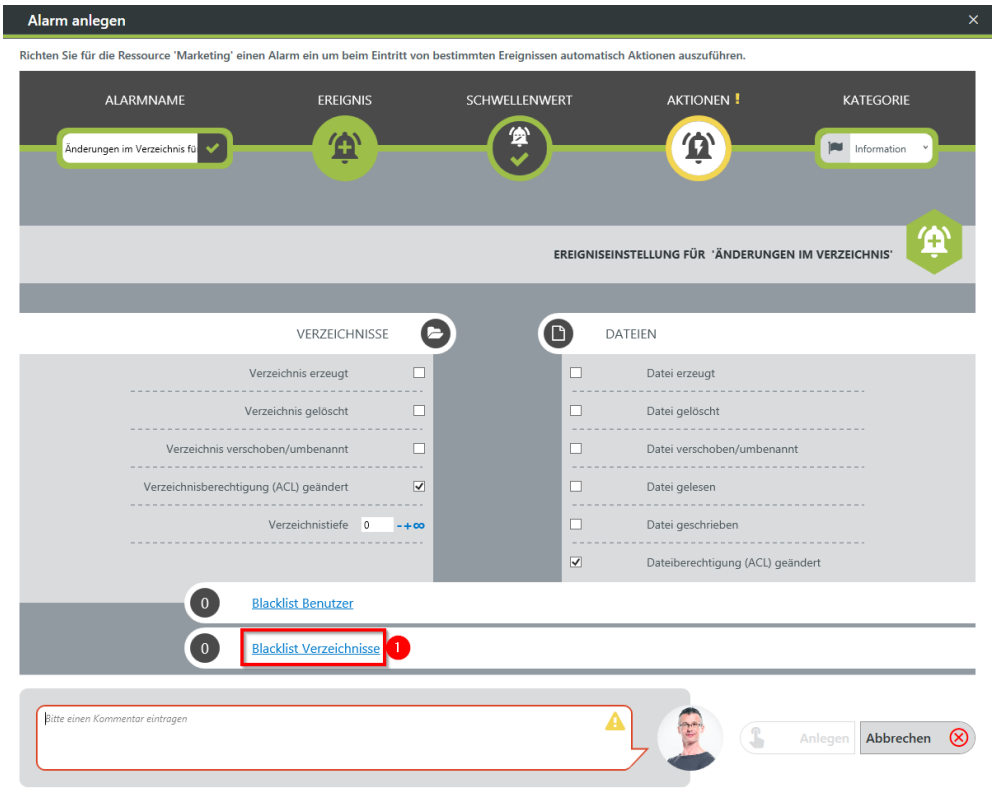
Optional:

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

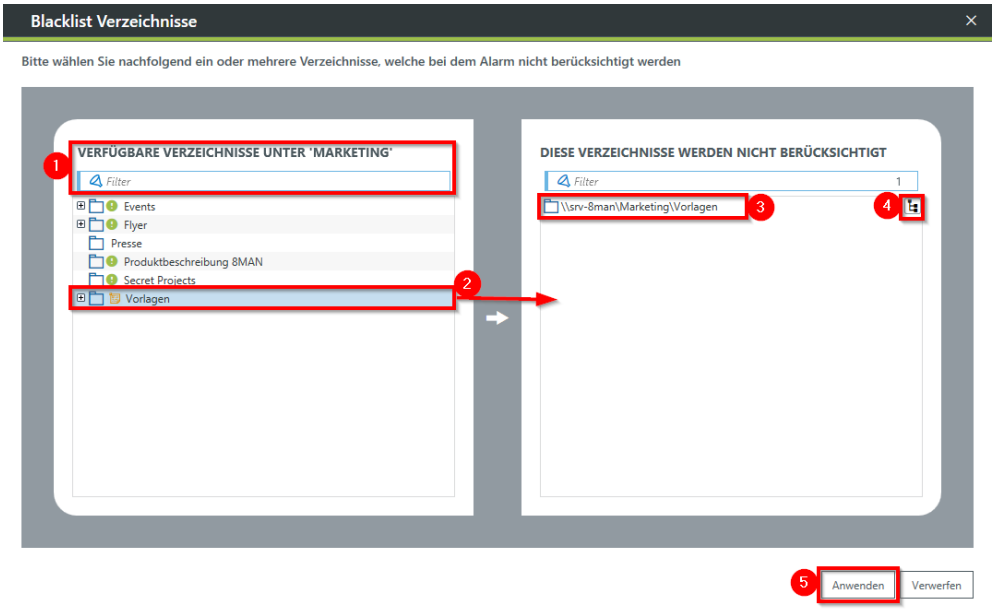
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

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.*



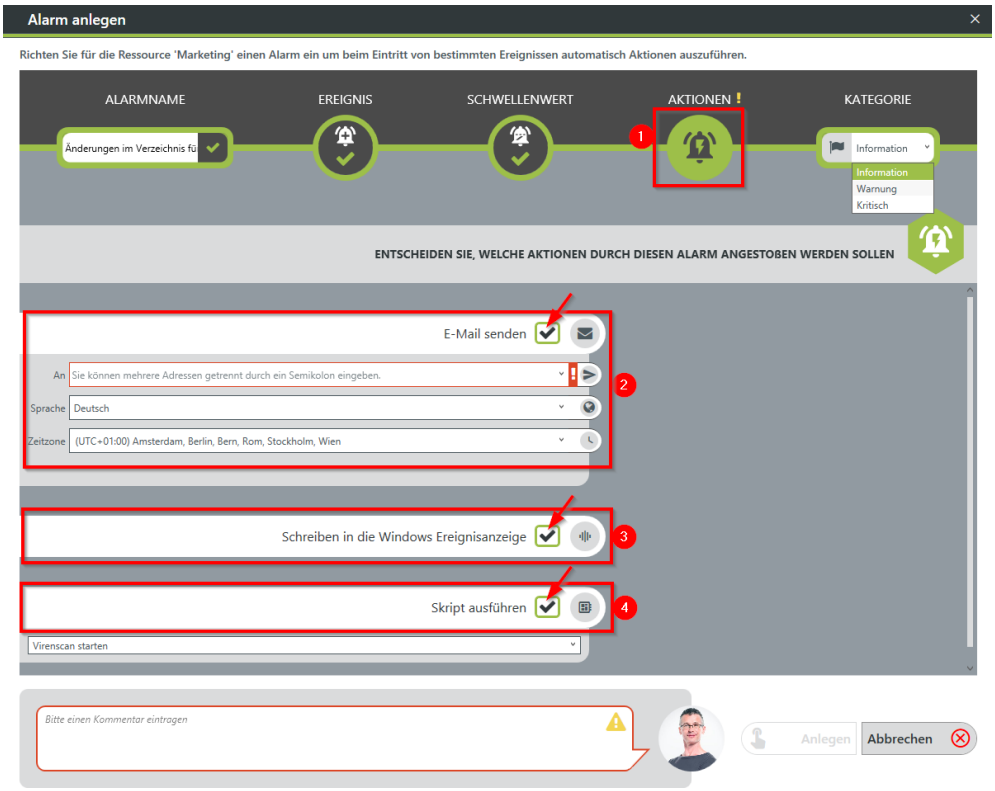
1. *Optional: Wählen Sie "Blacklist Verzeichnisse".*



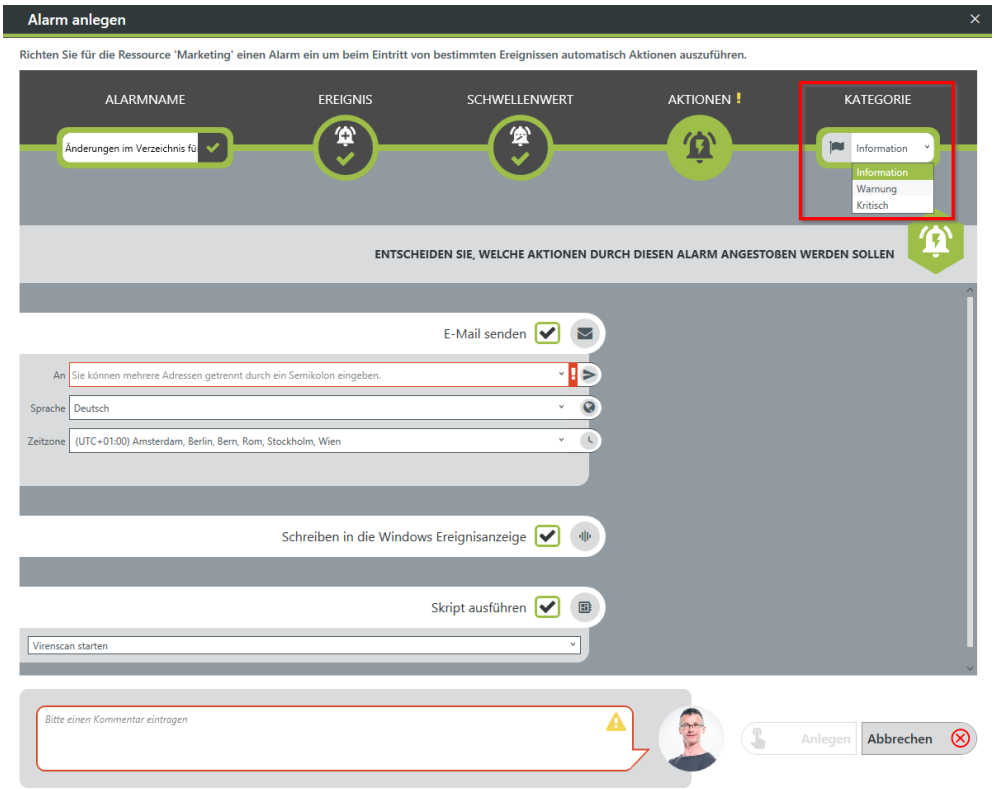
Optional:

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.*

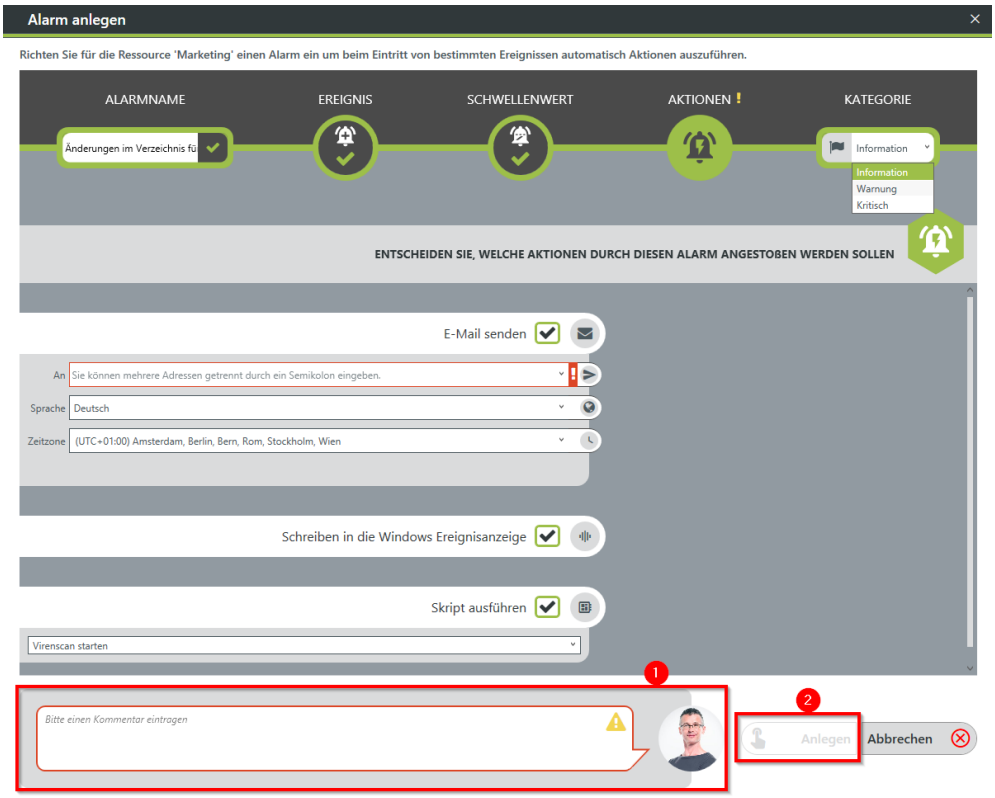


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll.*
   Der Inhalt der E-Mails kann angepasst werden. 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".*

4.1.2 Alarme für Verdachtsfälle auf Datendiebstahl aktivieren (Fileserver)

Hintergrund / Mehrwert

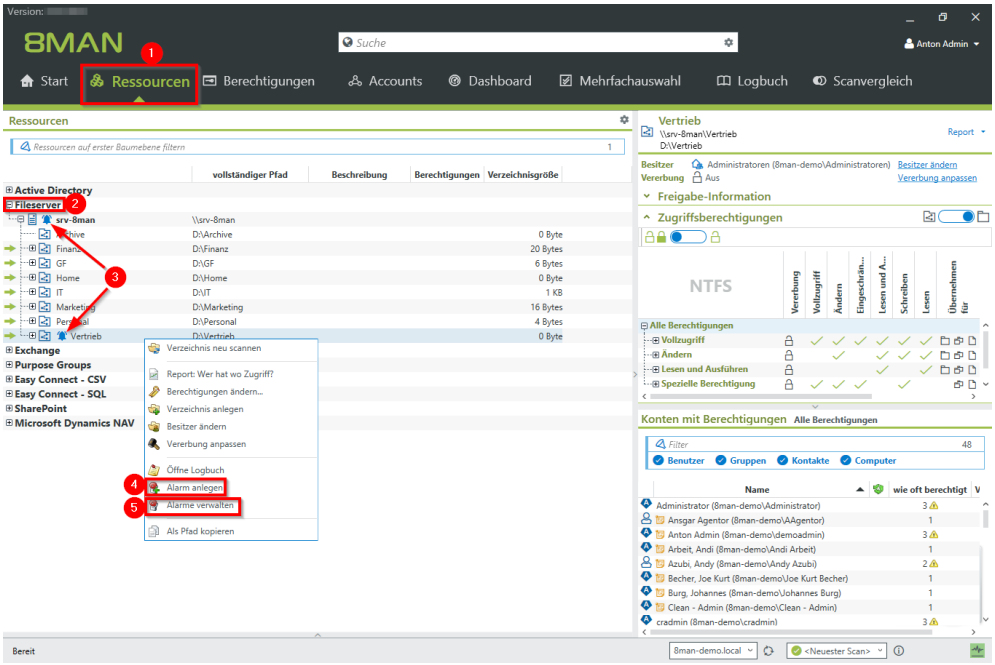
Um Sicherheitsvorfälle effizient zu erfassen, nimmt 8MAN die von Nutzern ausgelösten Fileserver-Events in den Blick. Treten diese in ungewohnt hoher Zahl und zusätzlich in einem kurzen Zeitraum auf, informiert 8MAN proaktiv alle Verantwortlichen.

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

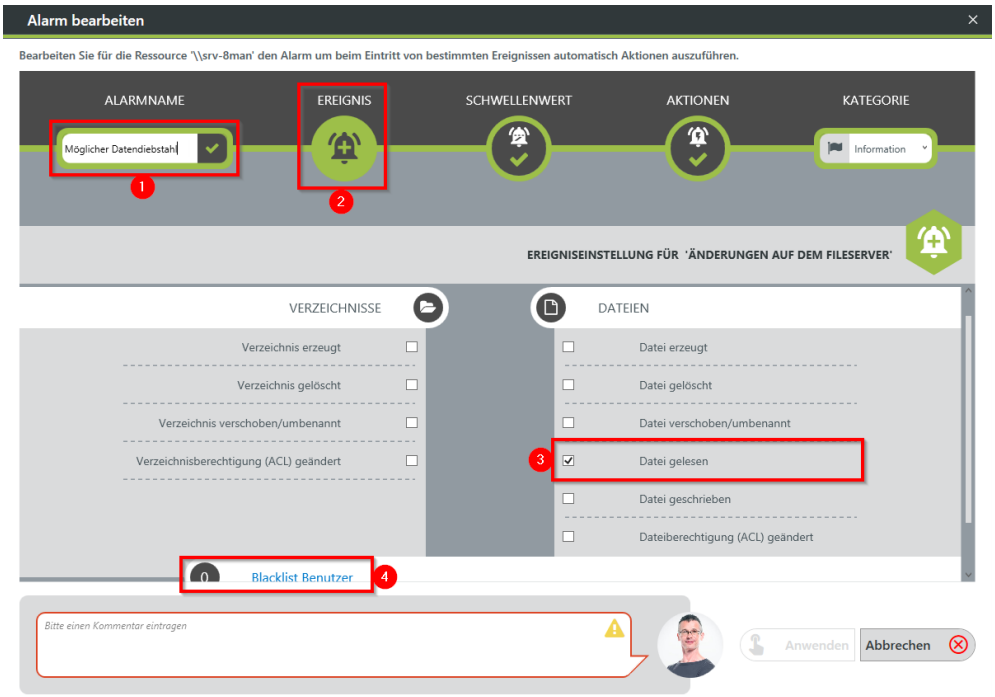
Weiterführende Services

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

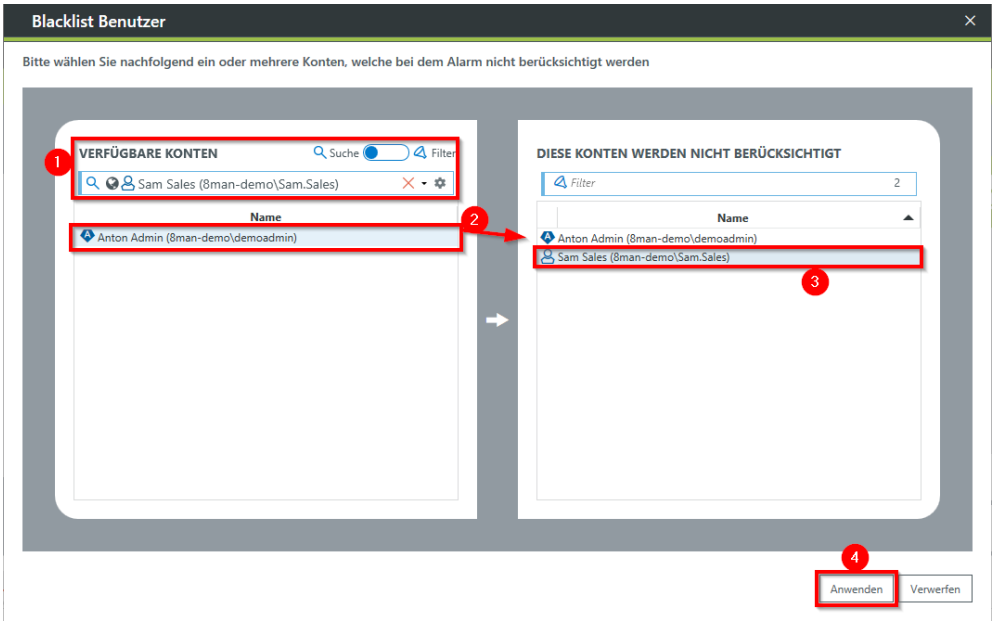
Der Prozess in einzelnen Schritten



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".*



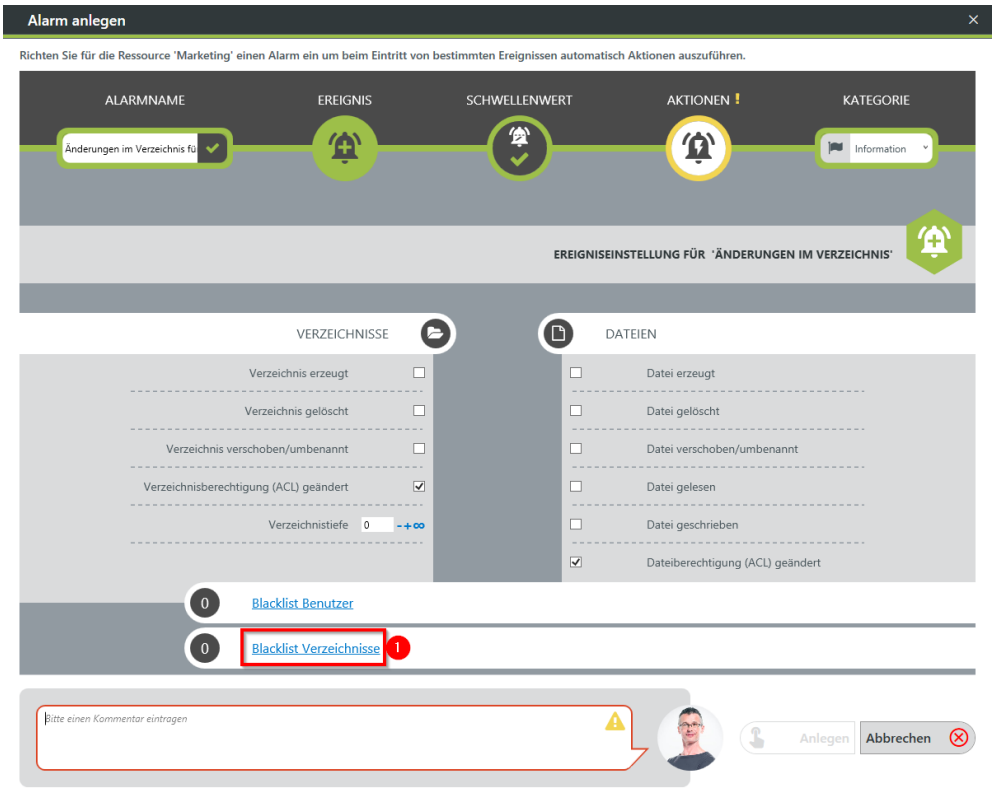
Optional:

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

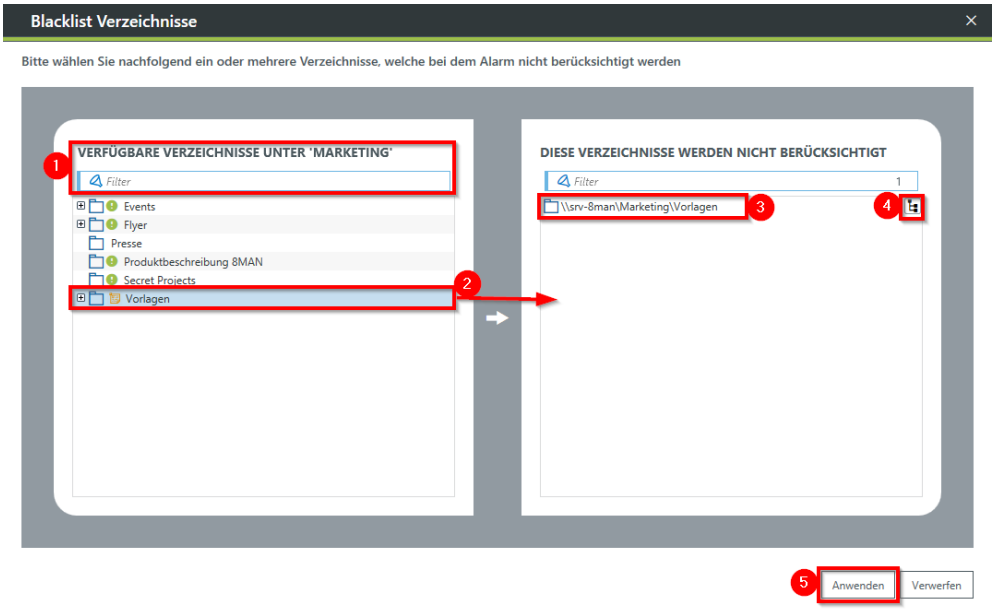
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

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.*



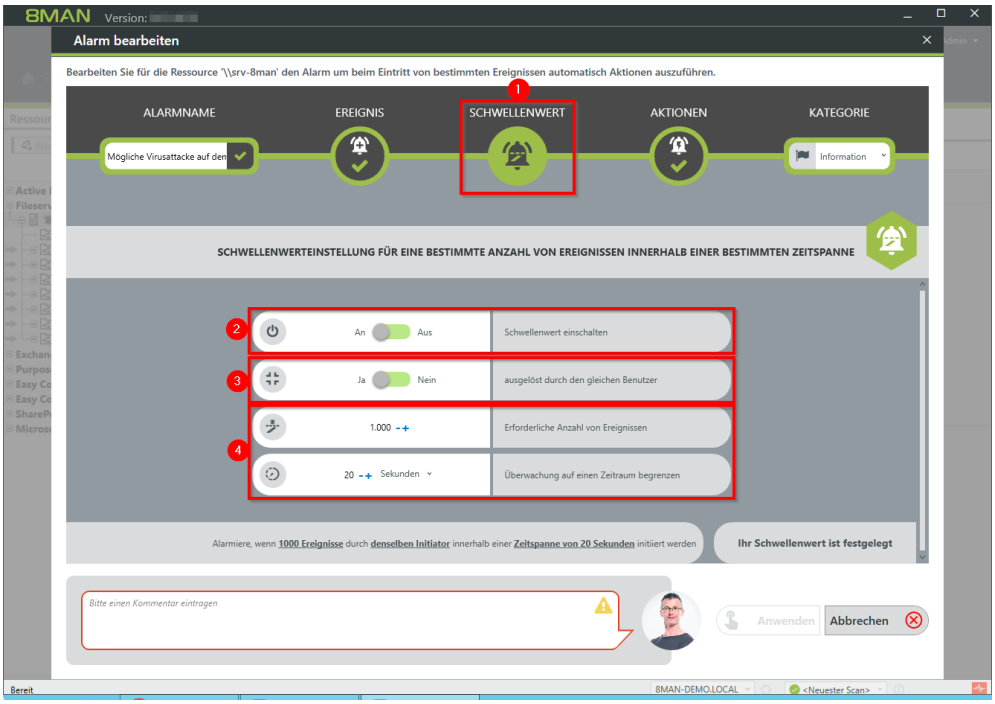
1. *Wählen Sie "Blacklist Verzeichnisse".*



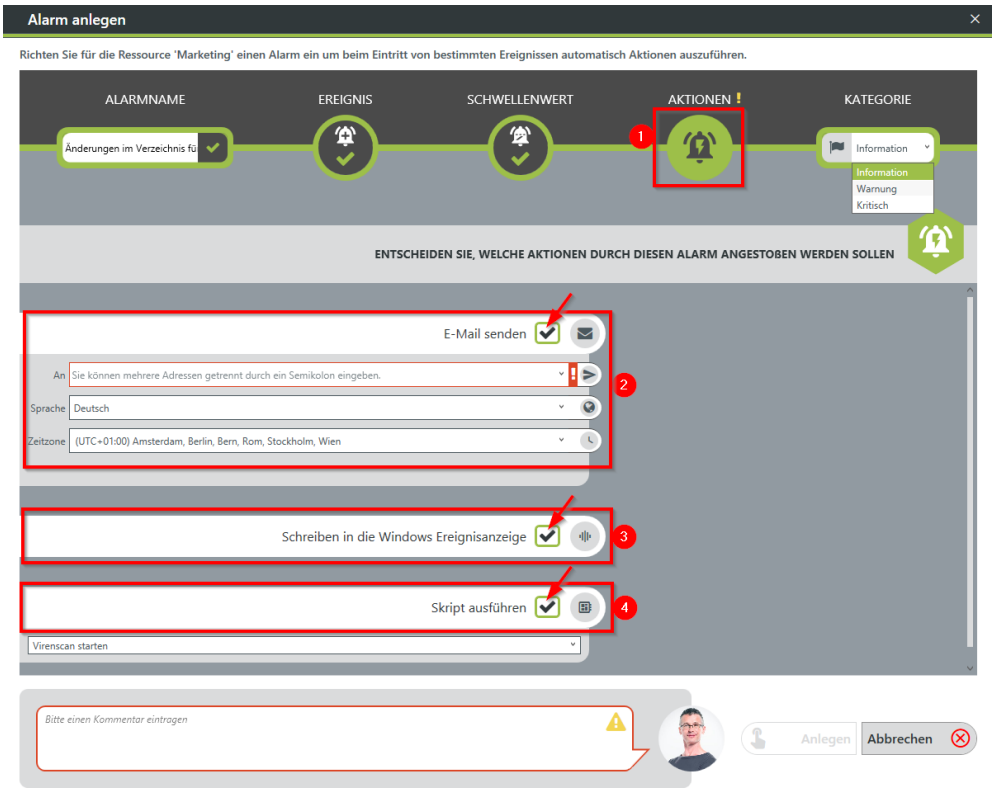
Optional:

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

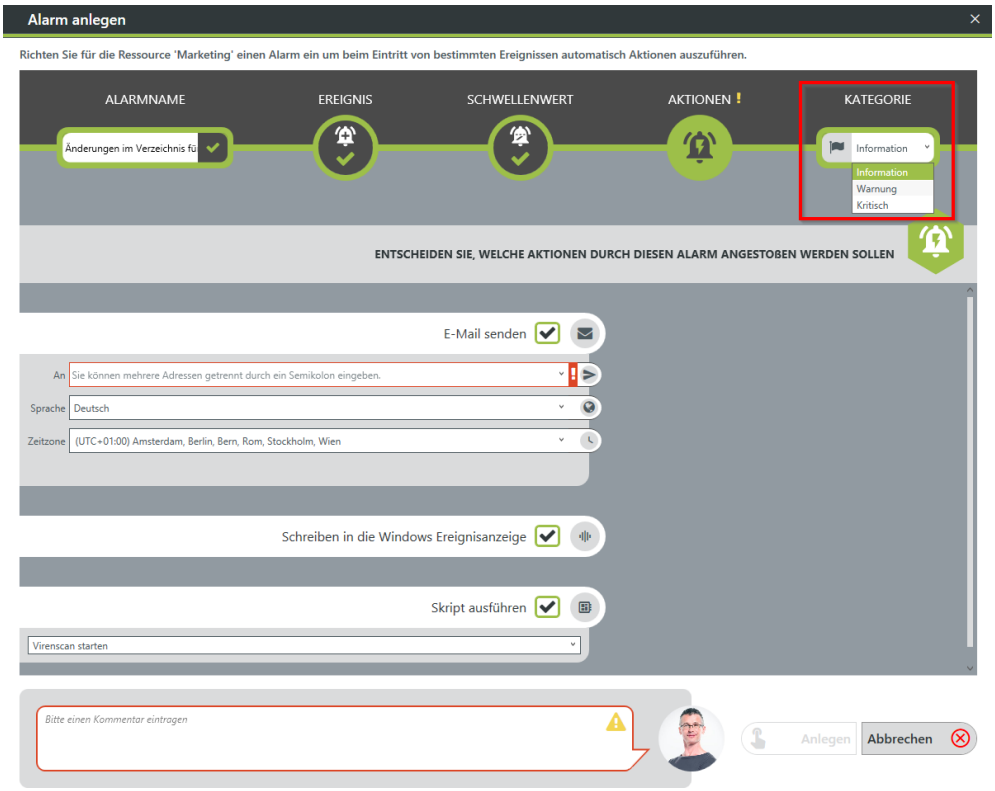
1. *Nutzen Sie die Filterfunktion, um die gewünschten Verzeichnisse zu finden. Wenn Sie filtern, ändert sich die Baumansicht zu einer Ergebnisliste der Verzeichnispfade.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Verzeichnisse zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Verzeichnisse 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.*

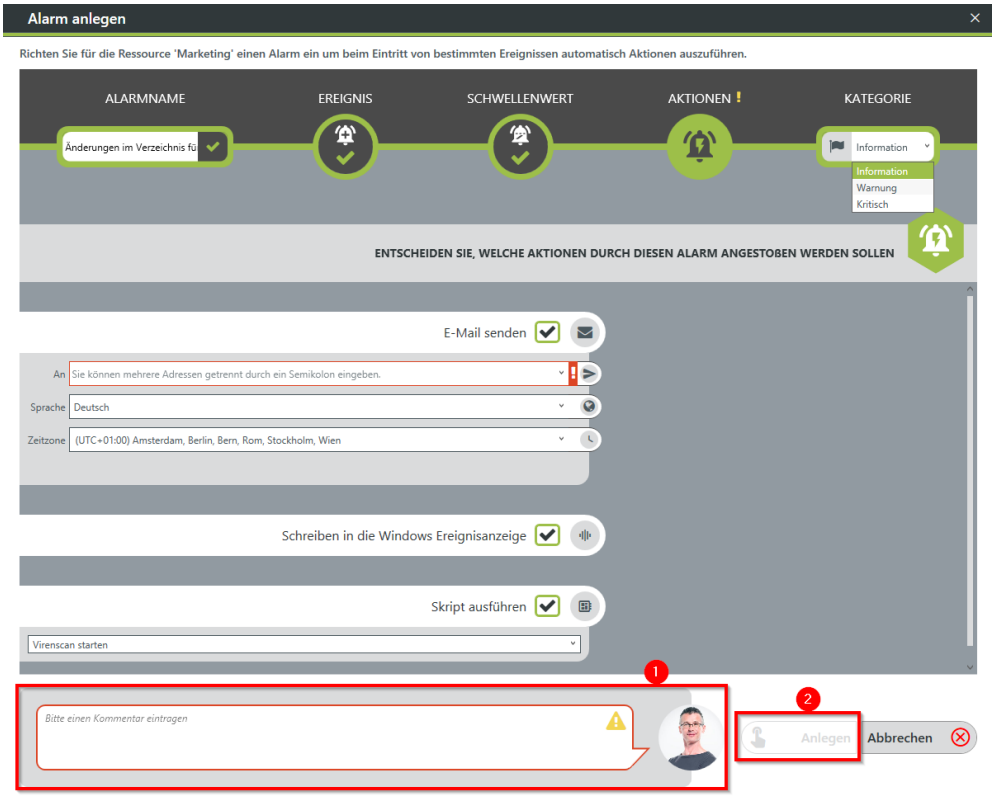


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll.*
   Der Inhalt der E-Mails kann angepasst werden. 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".*

4.1.3 Alarme für Datenlöschungen aktivieren (Fileserver)

Hintergrund / Mehrwert

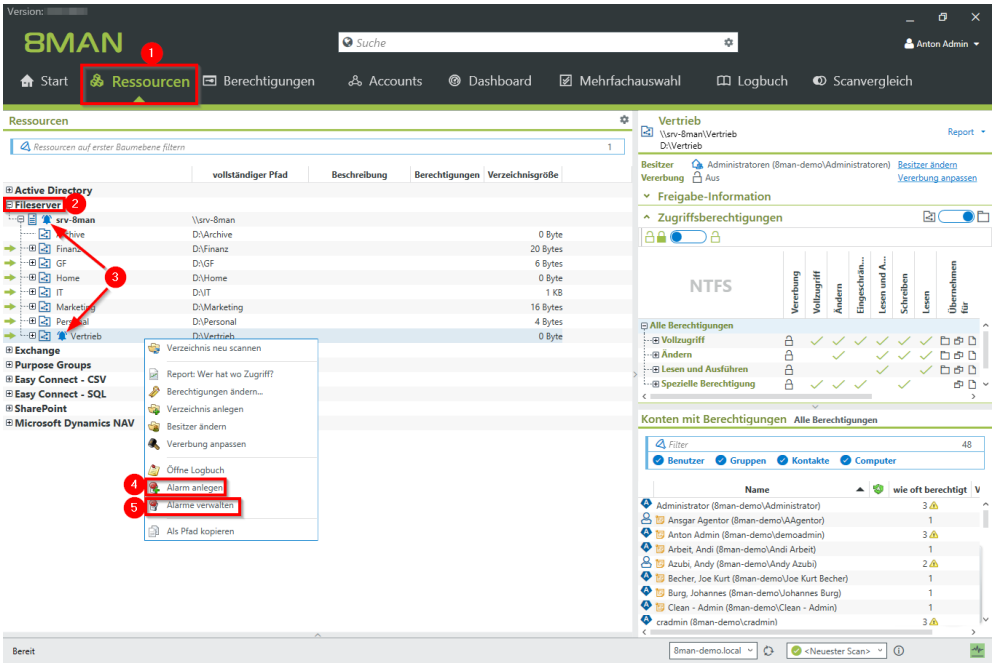
Um Sicherheitsvorfälle effizient zu erfassen, nimmt 8MAN die von Nutzern ausgelösten Fileserver-Events in den Blick. Treten diese in ungewohnt hoher Zahl und zusätzlich in einem kurzen Zeitraum auf, informiert 8MAN proaktiv alle Verantwortlichen.

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

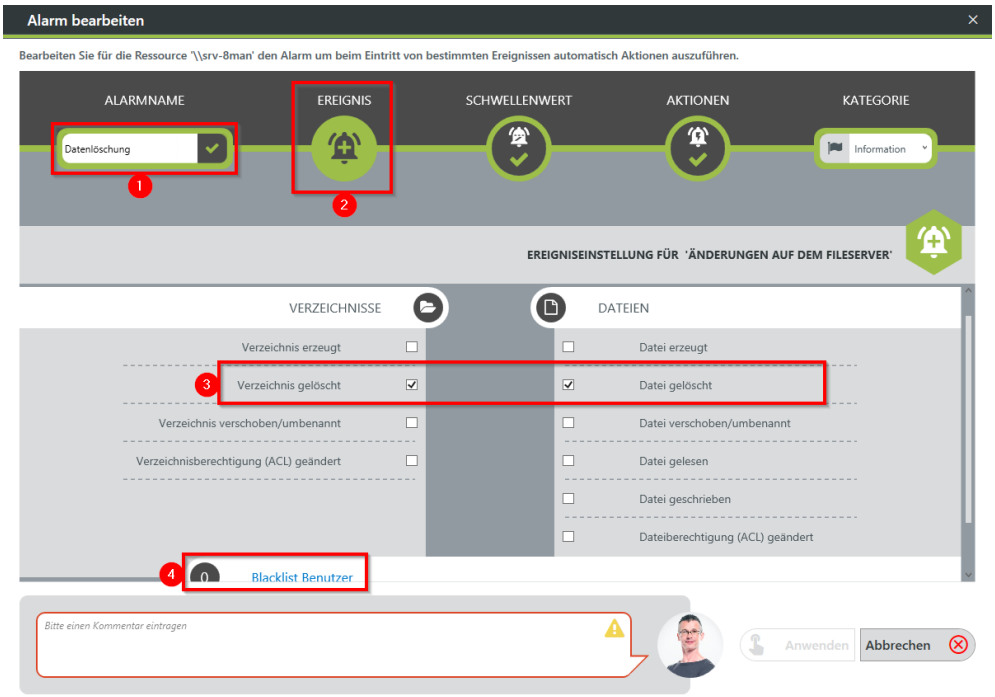
Weiterführende Services

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

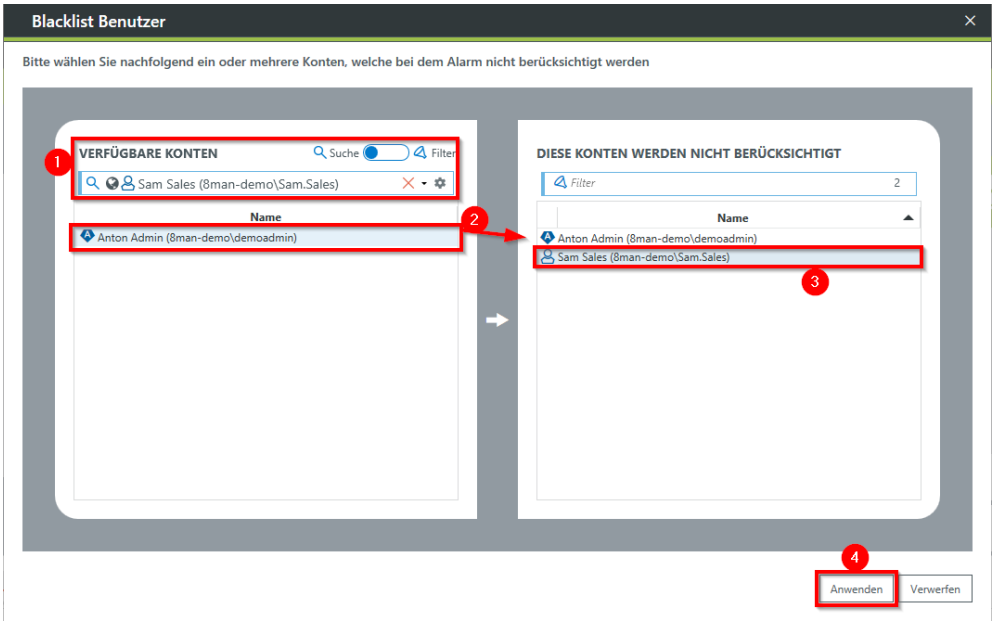
Der Prozess in einzelnen Schritten



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".*



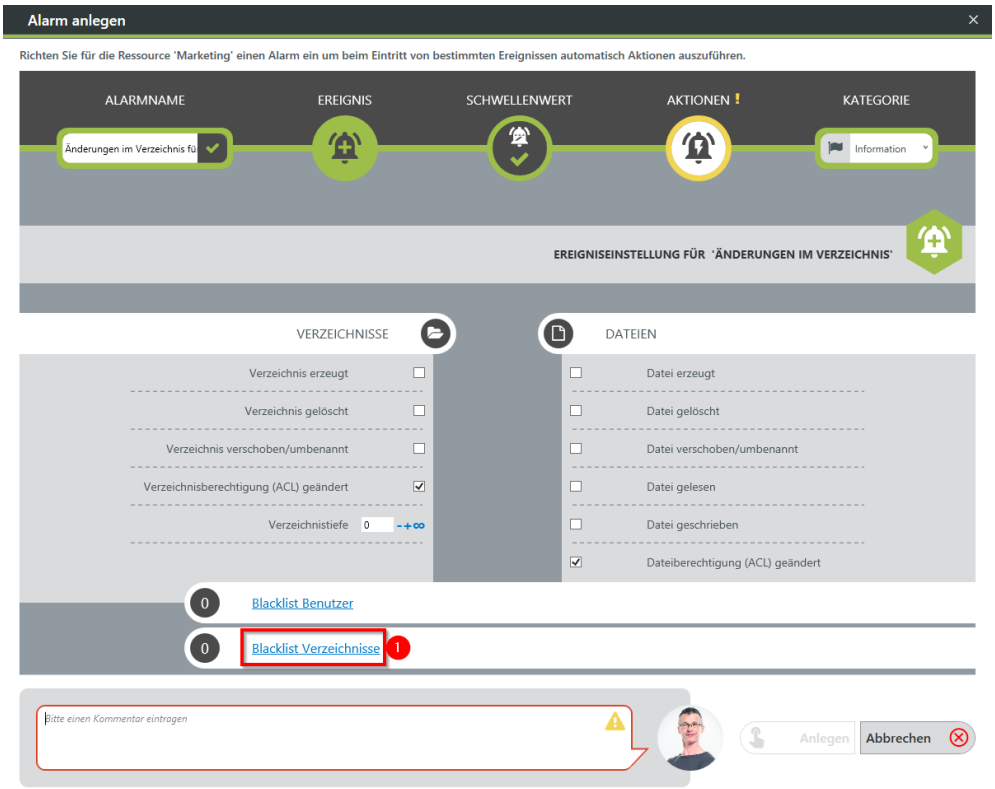
Optional:

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

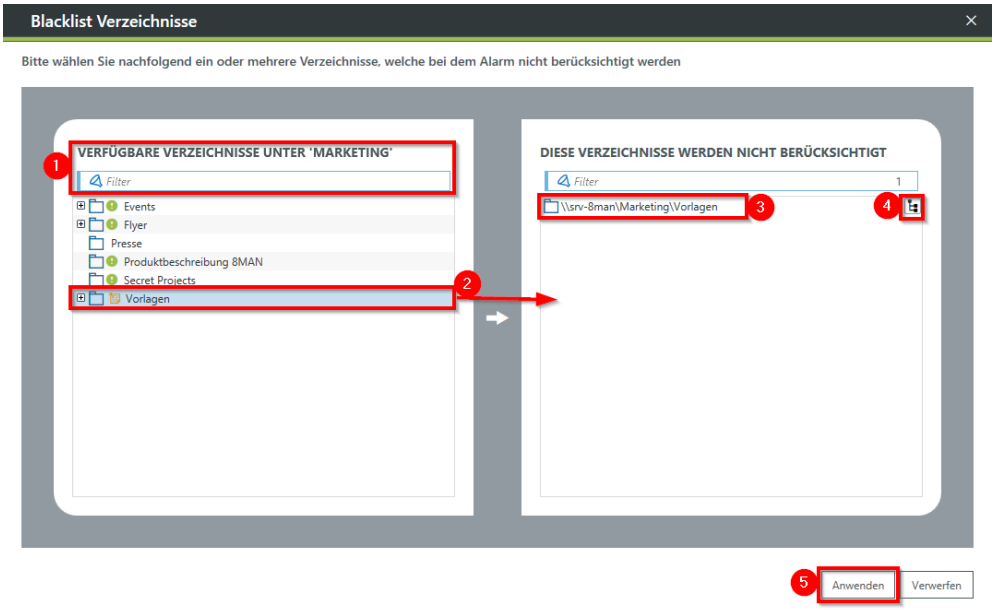
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

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.*



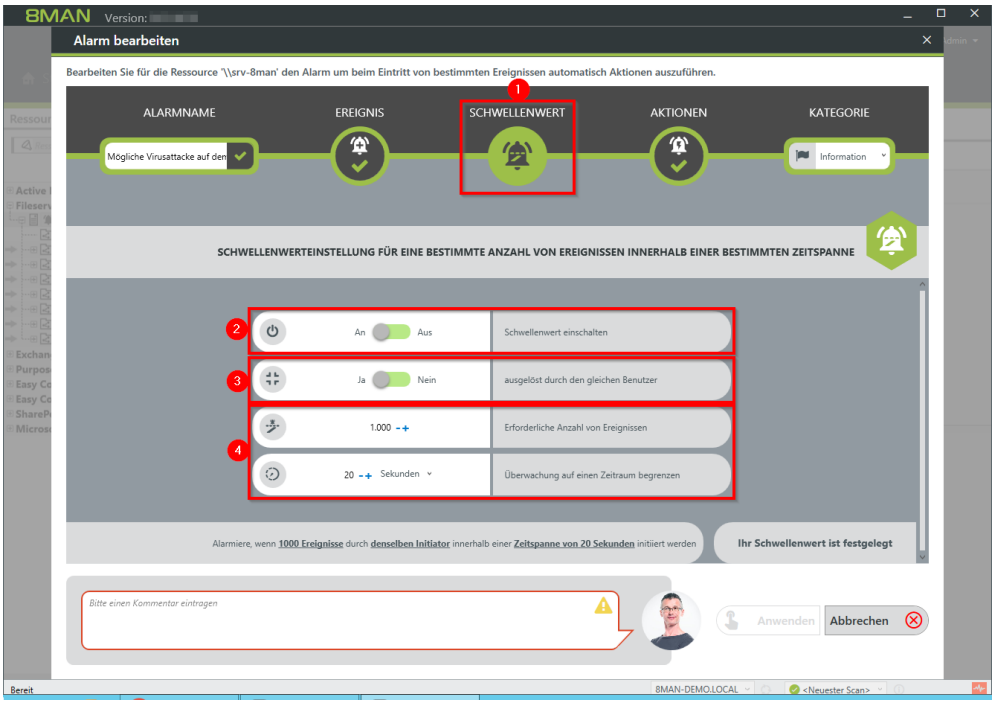
1. *Wählen Sie "Blacklist Verzeichnisse".*



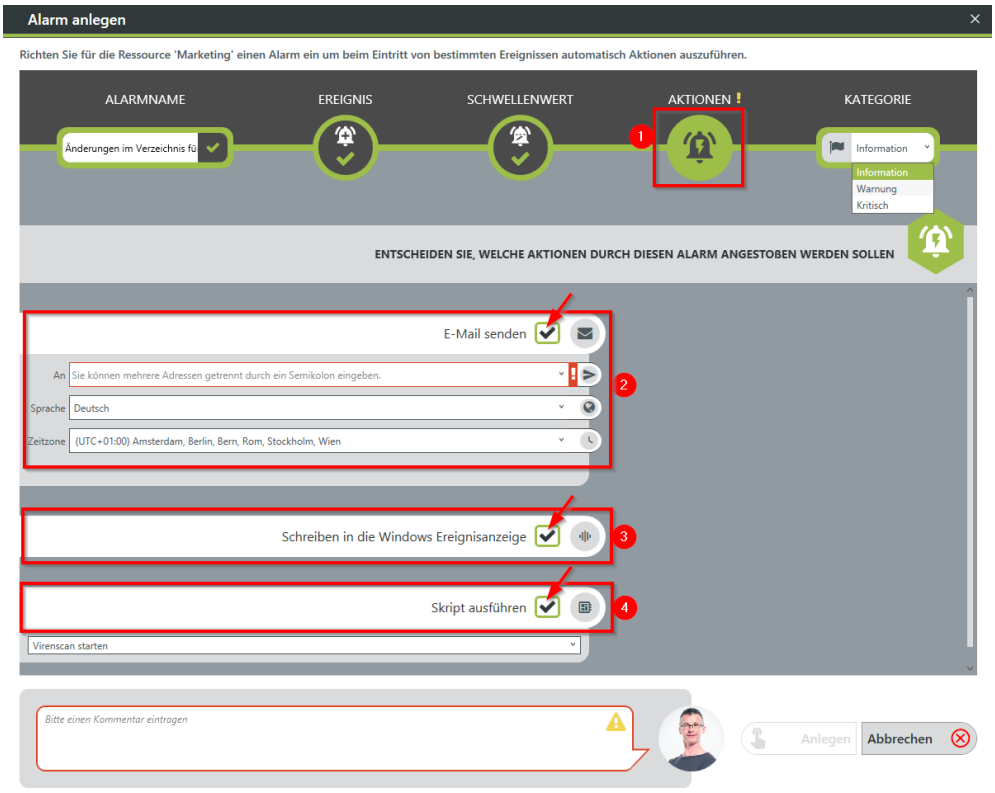
Optional:

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

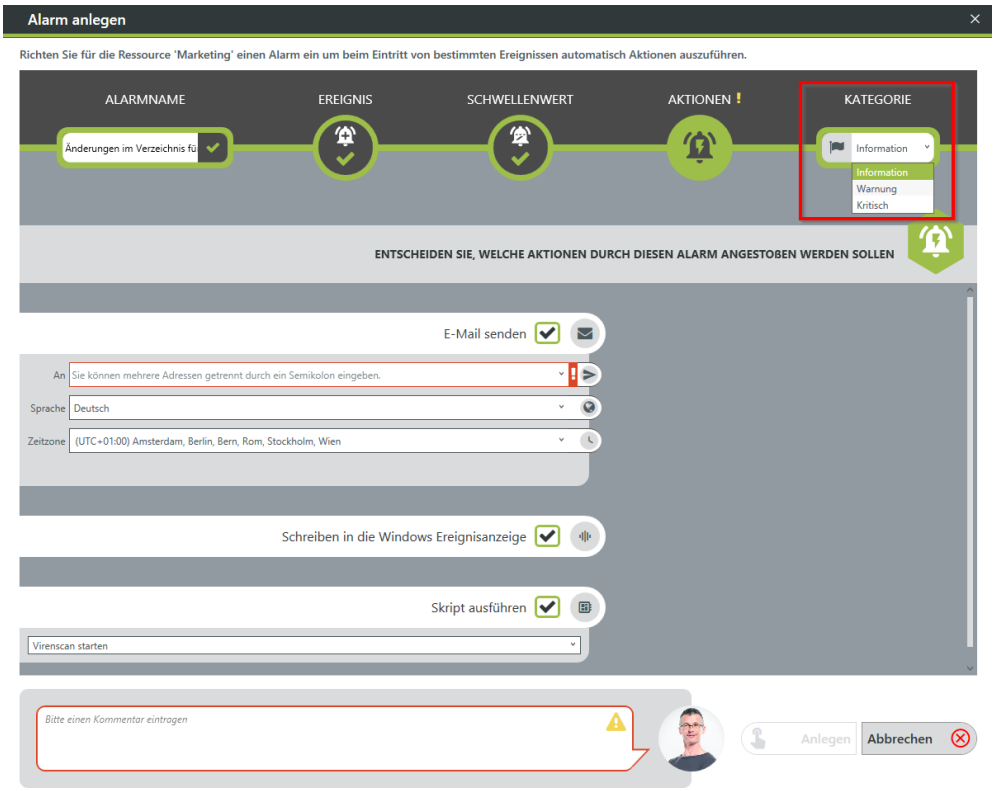
1. *Nutzen Sie die Filterfunktion, um die gewünschten Verzeichnisse zu finden. Wenn Sie filtern, ändert sich die Baumansicht zu einer Ergebnisliste der Verzeichnispfade.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Verzeichnisse zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Verzeichnisse 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.*

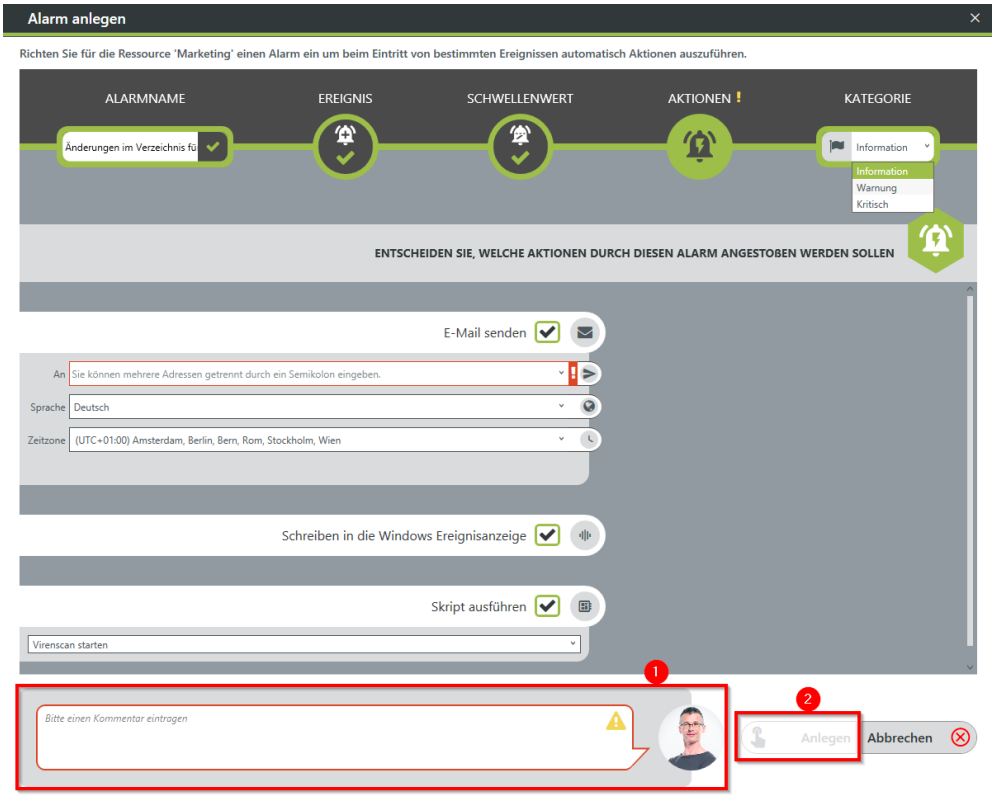


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll. Der Inhalt der E-Mails kann angepasst werden. 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".*

4.1.4 Alarme für Verdachtsfälle auf Ransomware aktivieren (Fileserver)

Hintergrund / Mehrwert

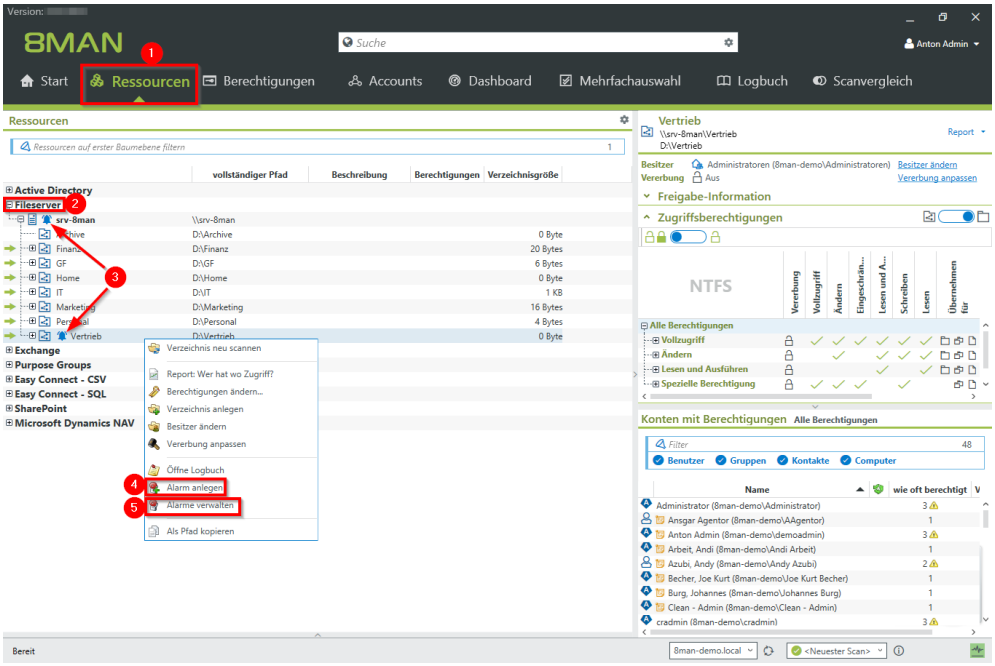
Um Sicherheitsvorfälle effizient zu erfassen, nimmt 8MAN die von Nutzern ausgelösten Fileserver-Events in den Blick. Treten diese in ungewohnt hoher Zahl und zusätzlich in einem kurzen Zeitraum auf, informiert 8MAN proaktiv alle Verantwortlichen.

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

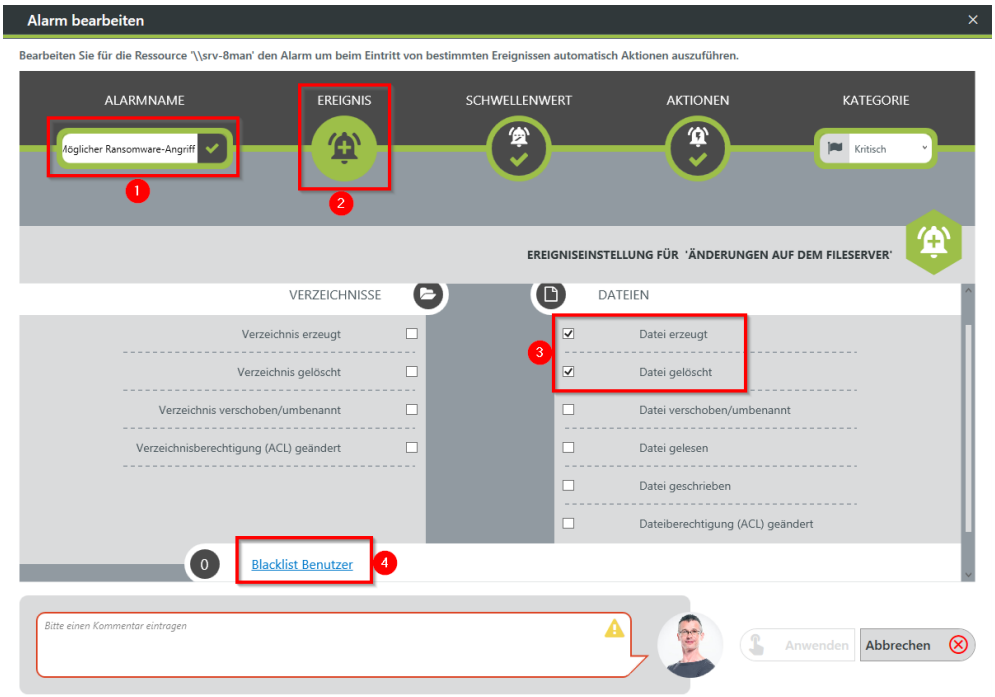
Weiterführende Services

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

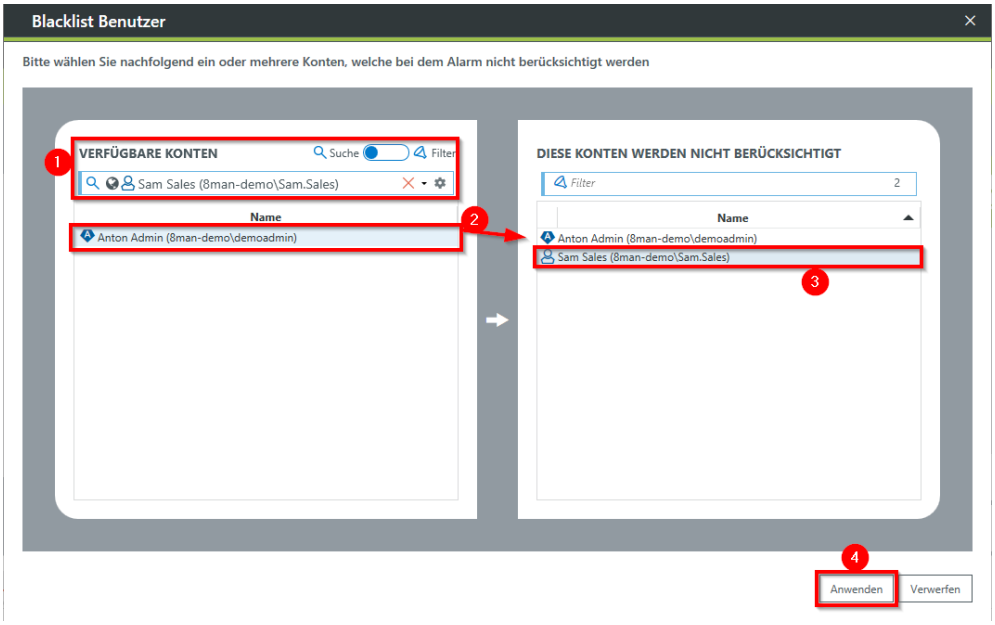
Der Prozess in einzelnen Schritten



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".*



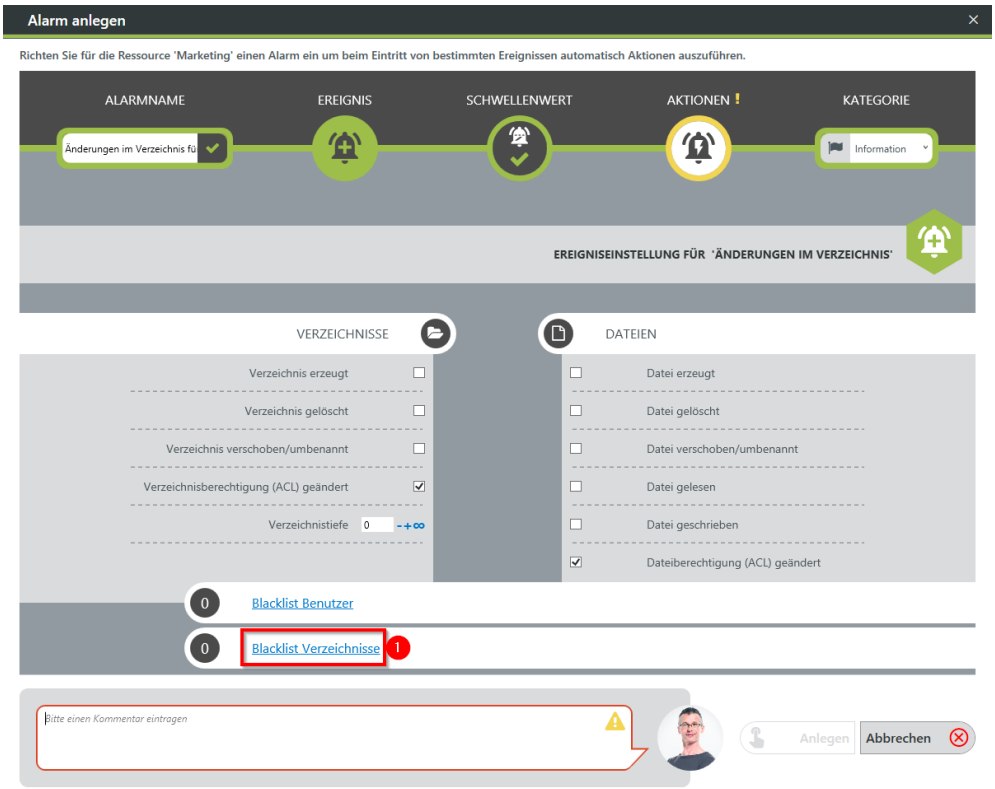
Optional:

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

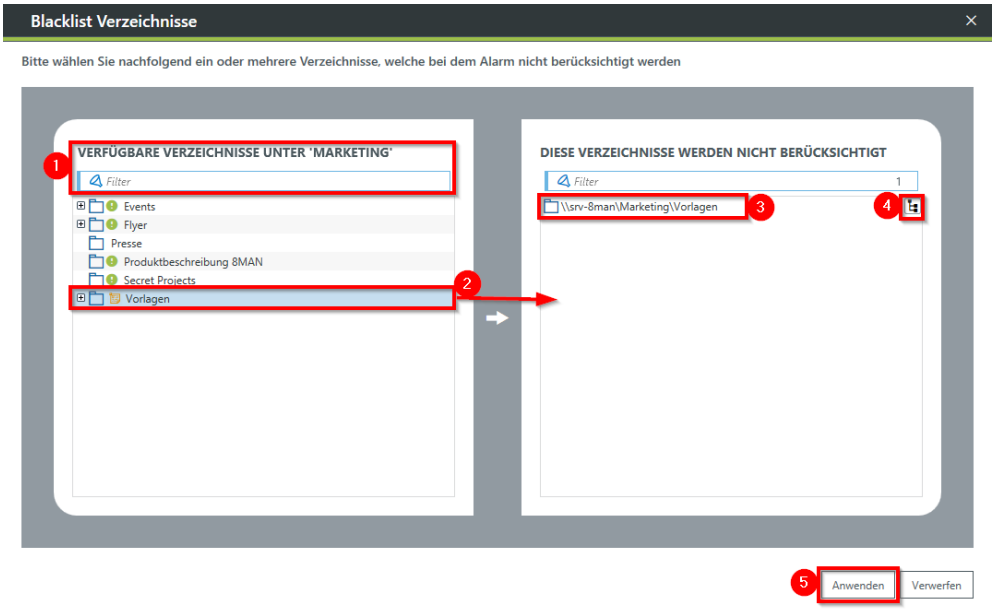
Jede Alarmkonfiguration hat ihre eigene Blacklistkonfiguration.

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.*



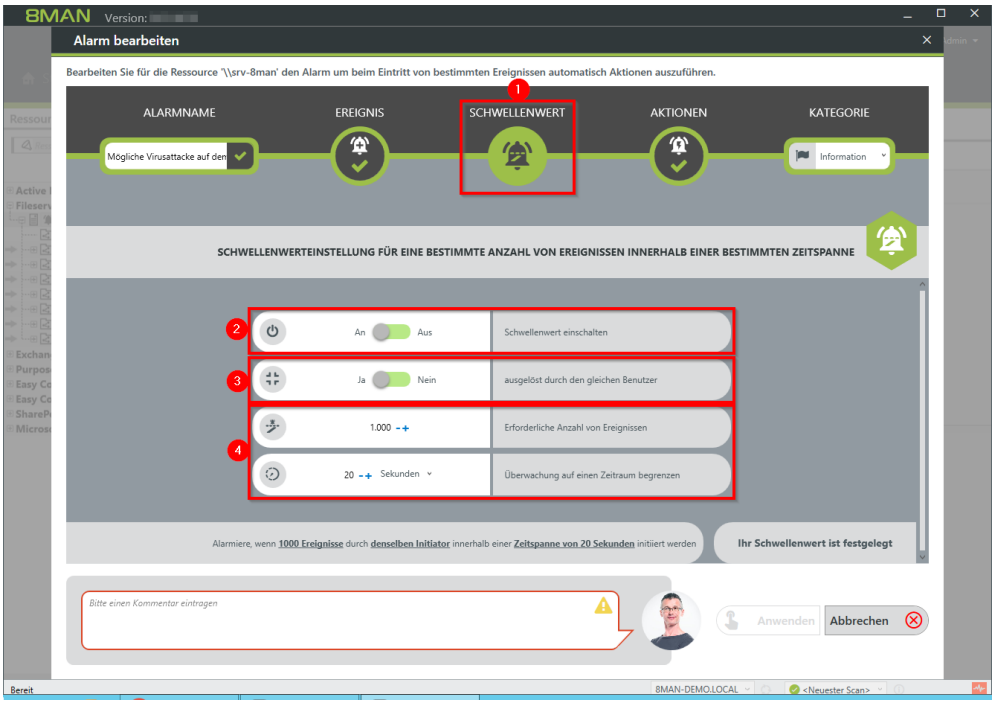
1. *Wählen Sie "Blacklist Verzeichnisse".*



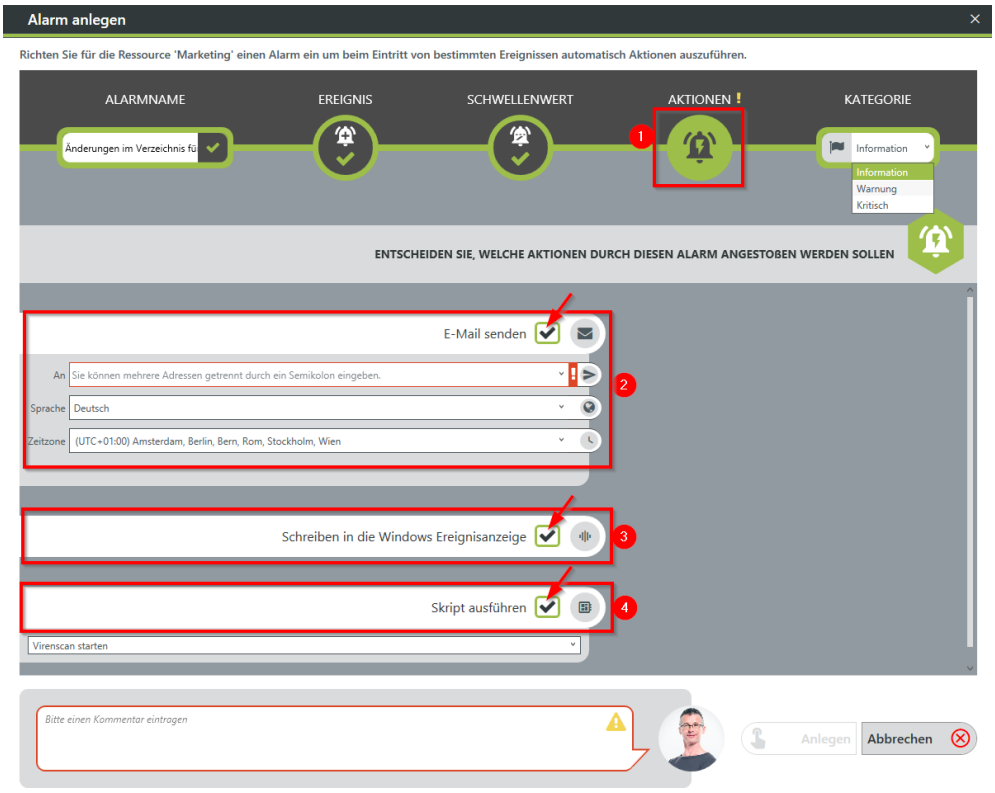
Optional:

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

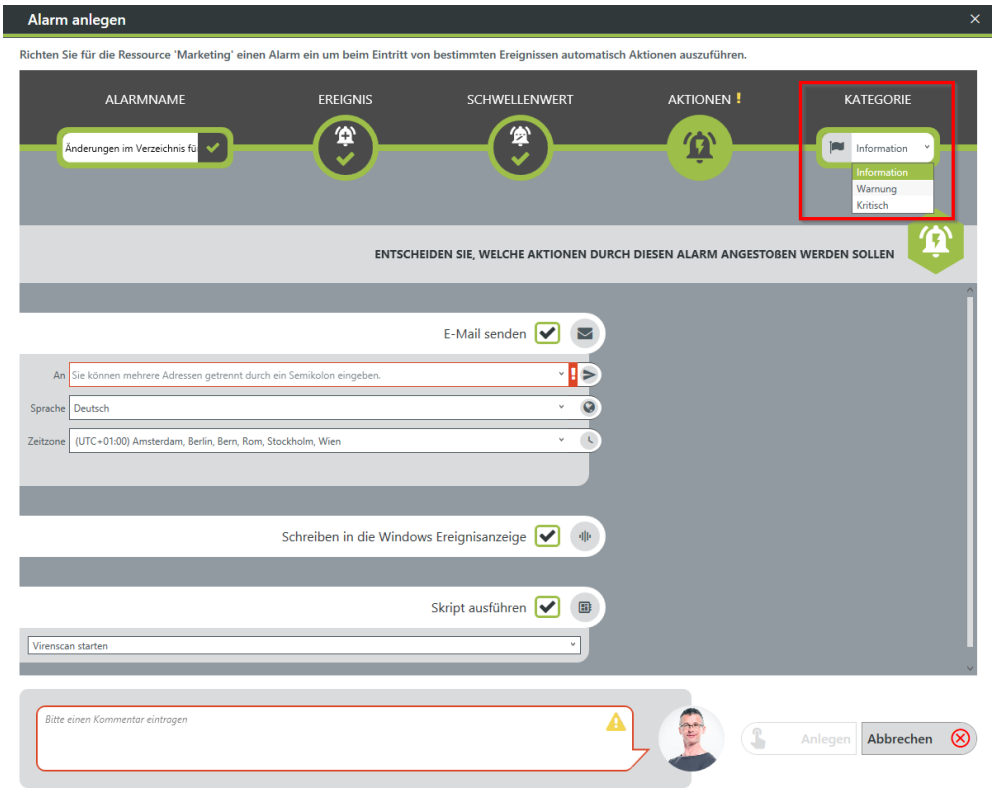
1. *Nutzen Sie die Filterfunktion, um die gewünschten Verzeichnisse zu finden. Wenn Sie filtern, ändert sich die Baumansicht zu einer Ergebnisliste der Verzeichnispfade.*
2. *Nutzen Sie Doppelklick oder Drag&Drop, um Verzeichnisse zur Blacklist hinzuzufügen.*
3. *Nutzen Sie die "Entf"-Taste, um Verzeichnisse 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.*

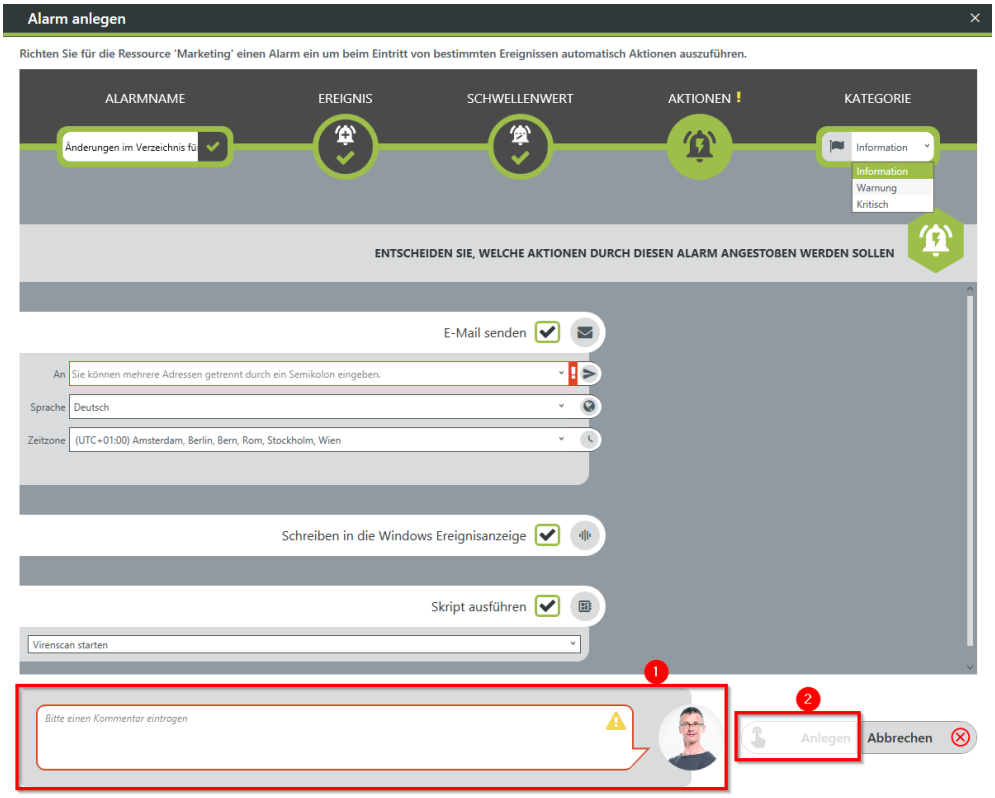


1. *Wählen Sie Aktionen. Hier legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Alarm ausgelöst wurde. Sie müssen mindestens eine Aktion aktivieren (Pfeile).*
2. *Aktivieren Sie die Option, wenn bei einem Alarm eine E-Mail versendet werden soll.*
   Der Inhalt der E-Mails kann angepasst werden. 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".*

4.1.5 Nach einem Alarm ein Skript ausführen

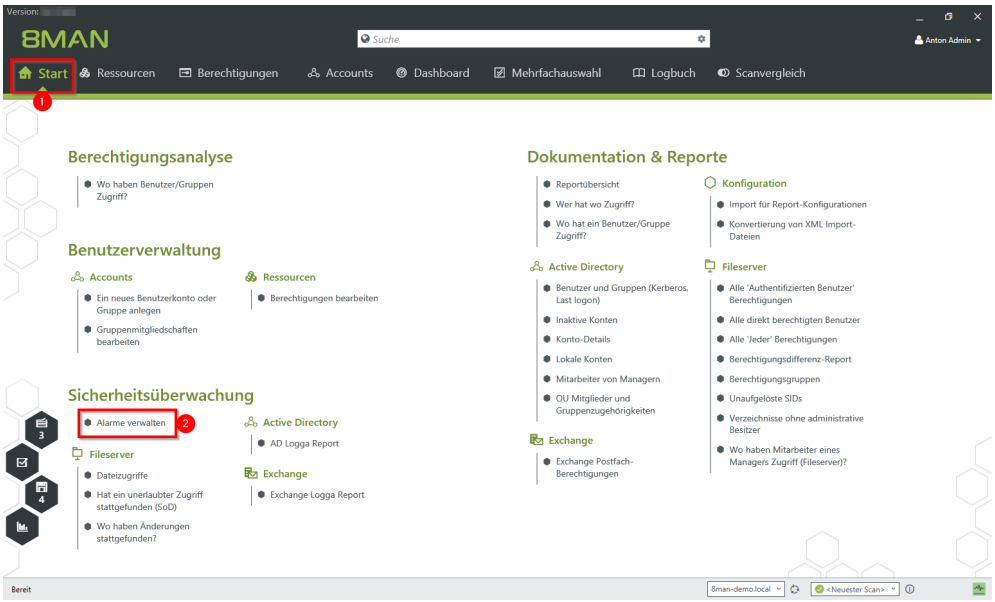
Hintergrund / Mehrwert

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.

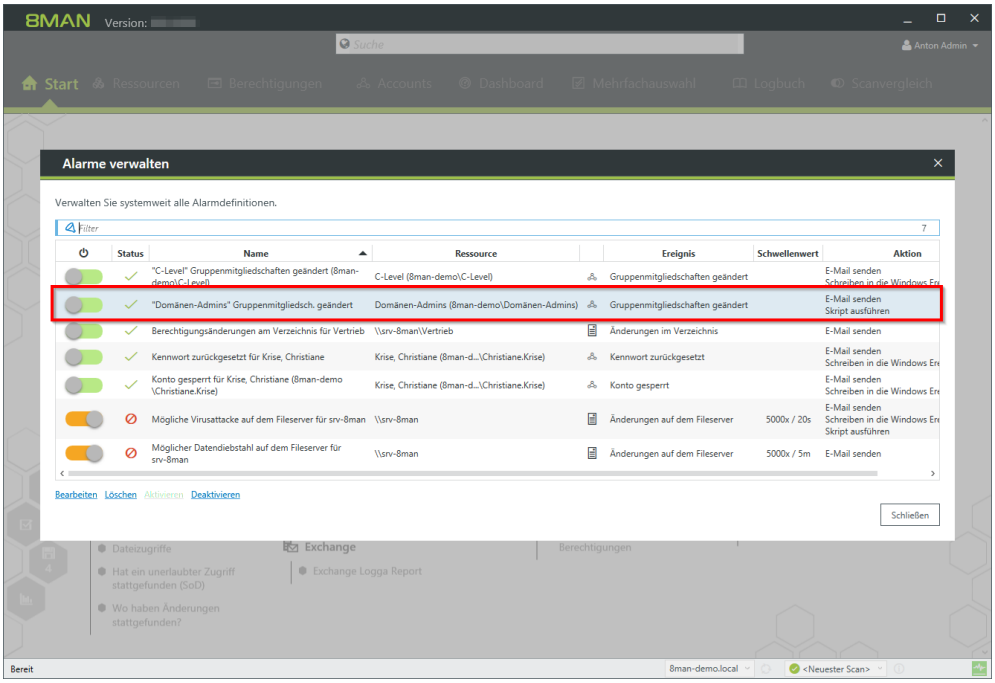
Weiterführende Services

Alarme verwalten

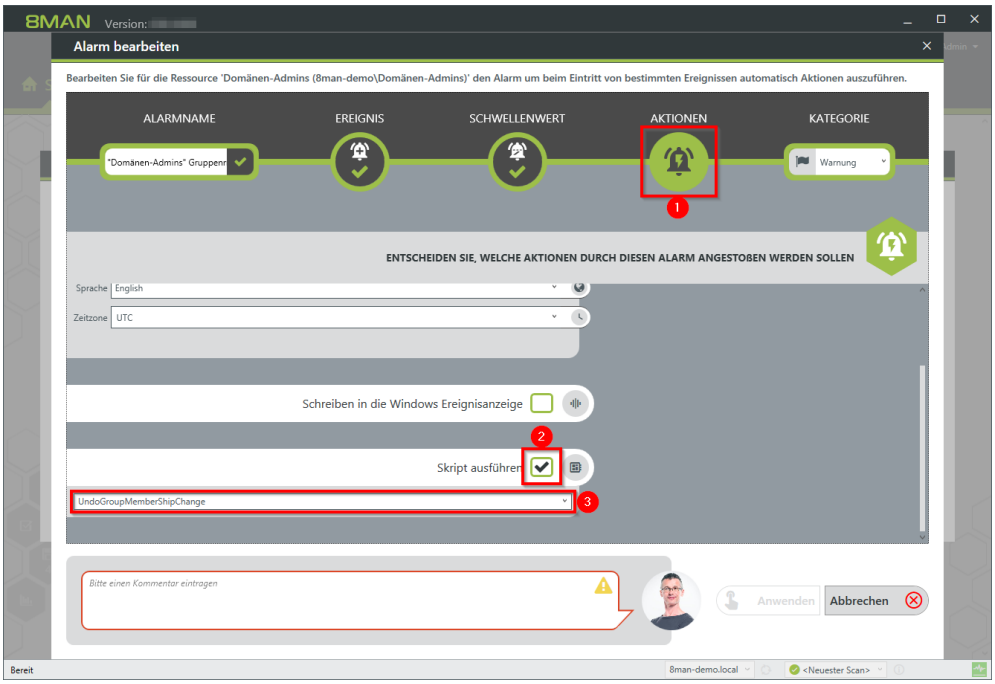
Der Prozess in einzelnen Schritten



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.

4.1.6 Alarme verwalten

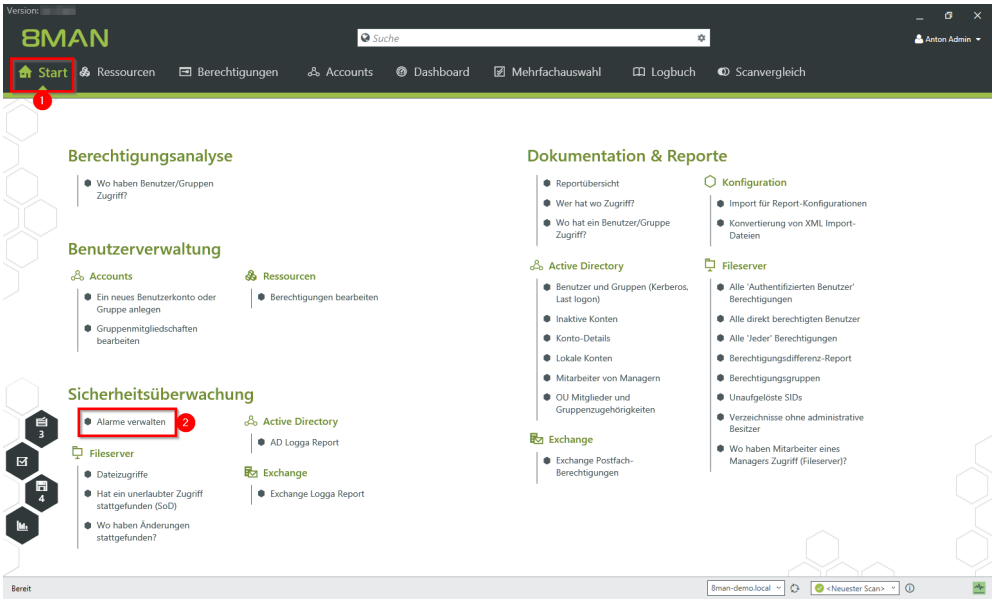
Hintergrund / Mehrwert

Passen Sie Alarme an veränderte Bedingungen an oder löschen Sie überflüssige Alarmkonfigurationen.

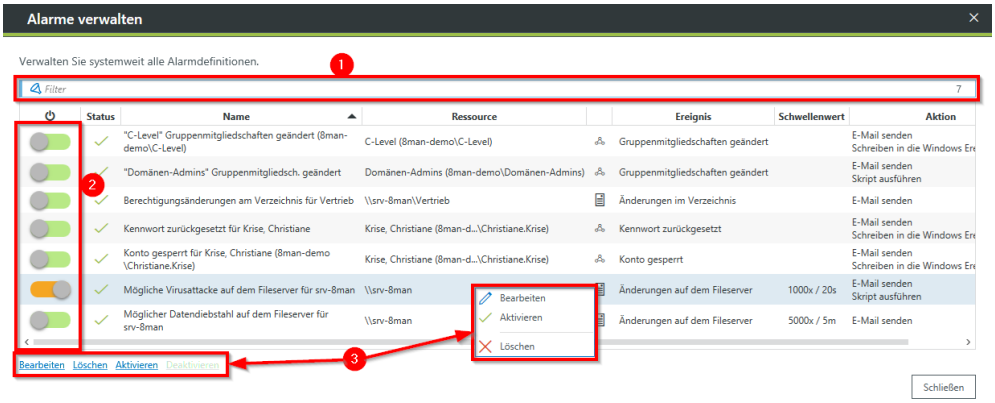
Weiterführende Services

Alarme für Fileserververzeichnisse aktivieren
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

Der Prozess in einzelnen Schritten



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



8MAN zeigt Ihnen alle Alarmkonfigurationen.

Mit einem Doppelklick auf einen Eintrag passen Sie eine Alarmkonfiguration an.

1. *Suchen Sie nach einer Alarmkonfiguration.*
2. *Schalten Sie Alarme ein oder aus.*
3. *Löschen Sie die selektierte Alarmkonfiguration.*

4.2 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)

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

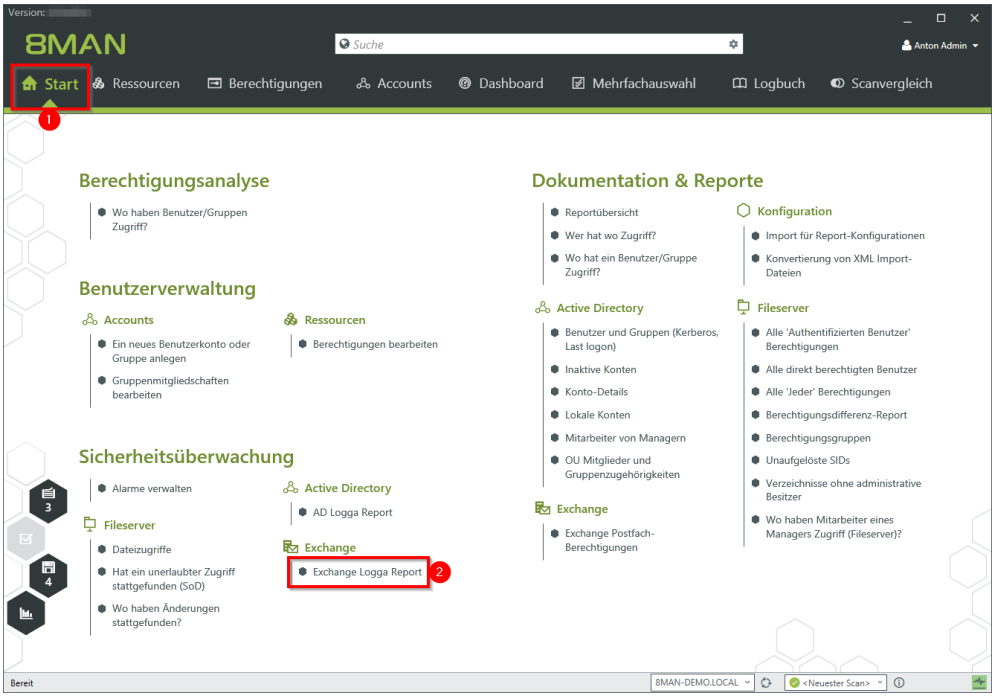
Hintergrund / Mehrwert

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.

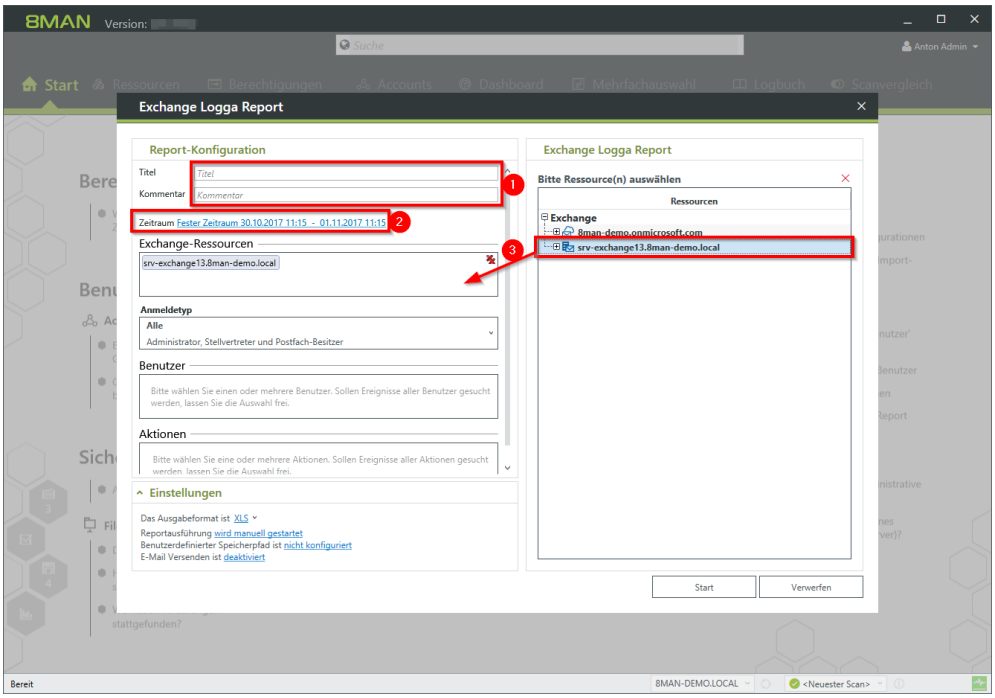
Weiterführende Services

Aktivitäten in Postfächern, Kalendern und Kontakten anzeigen (Logbuch)

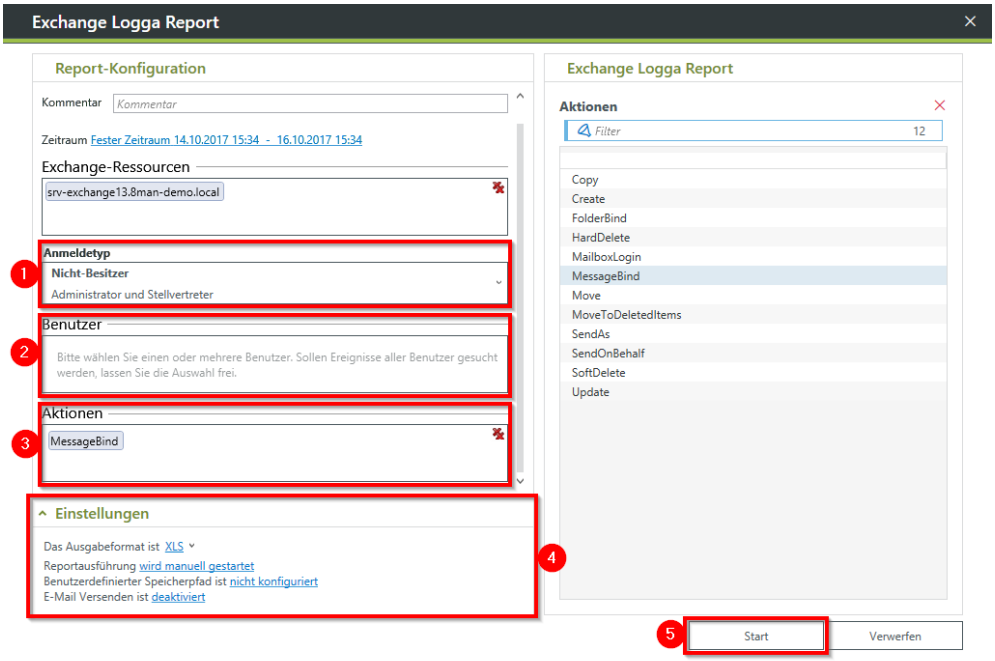
Der Prozess in einzelnen Schritten



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.*

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

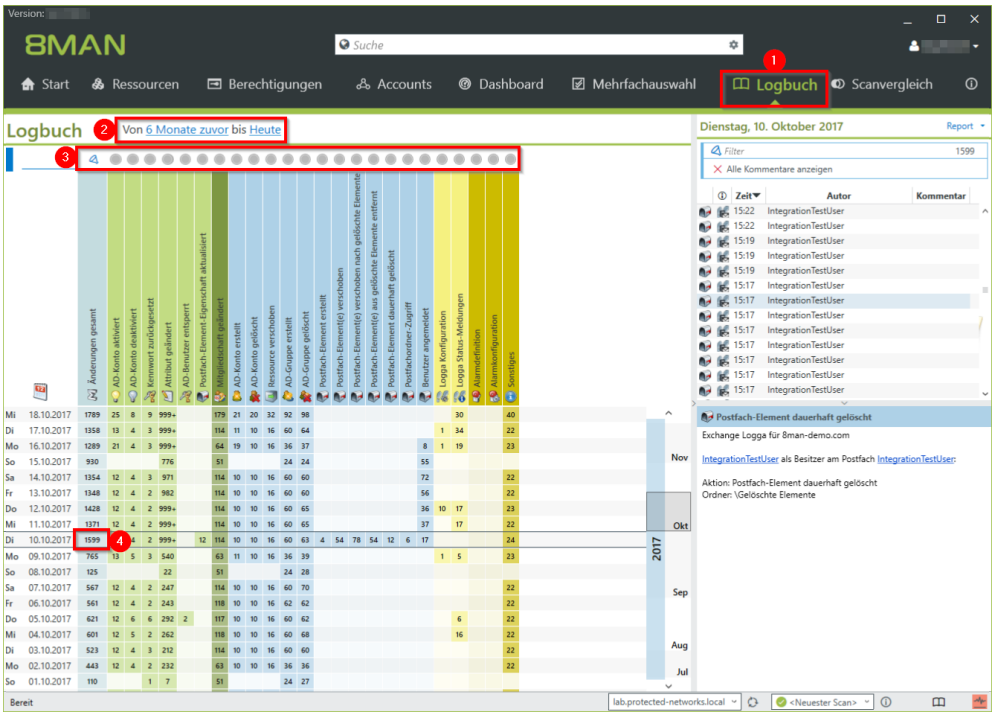
Hintergrund / Mehrwert

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.

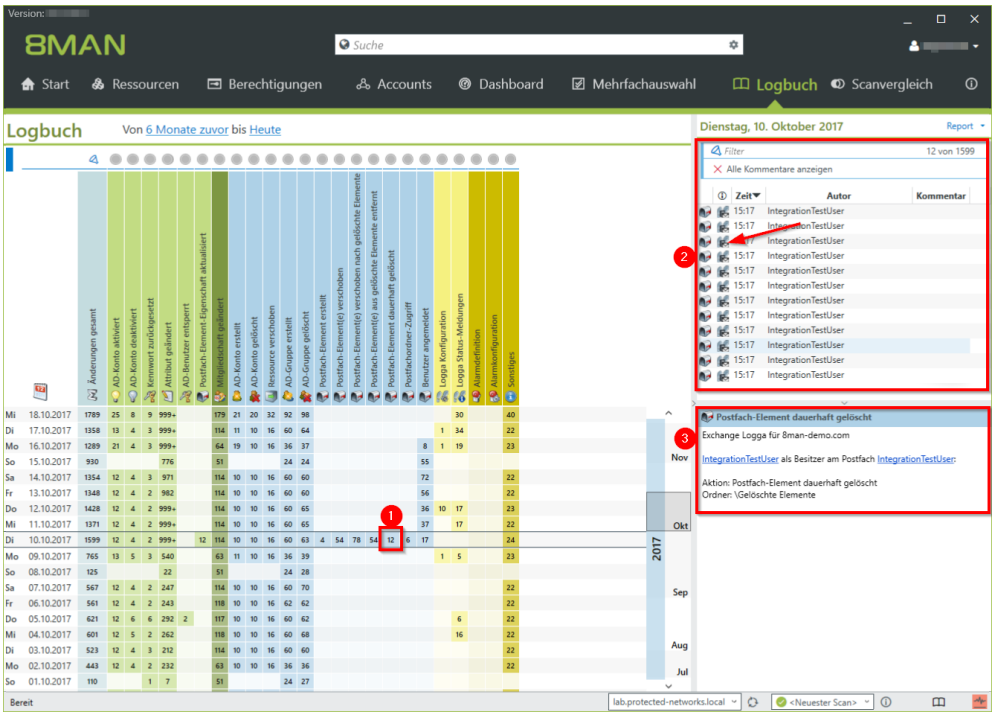
Weiterführende Services

Einen Report über Aktivitäten an Postfächern, Kalendern und Kontakten erstellen

Der Prozess in einzelnen Schritten



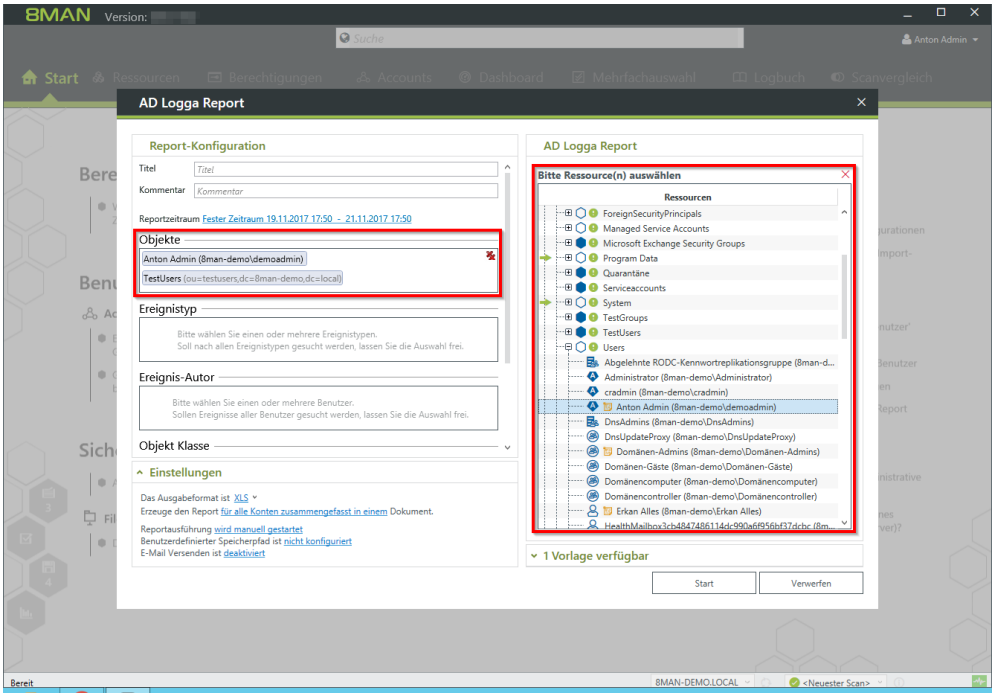
1. *Wählen Sie "Logbuch".*
2. *Legen Sie den Zeitraum für die Logbuch-Analyse fest.*
3. *Über die Filter fokussieren Sie auf die Events, die Sie prüfen möchten.*
4. *Selektieren Sie alle Ereignisse eines Tages (eine Zeile).*



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.*

4.3 AD Logga Report nach Objekten/OUs filtern

Der AD Logga Report erhält die Option, nach Objekten zu filtern. Dadurch wird es z. B. möglich einen Report zu erstellen, der nur Ereignisse einer OU enthält.



Filtern Sie den AD Logga Report nach AD Objekten, z. B. Benutzer oder OUs.

5 Role & Process Optimization

5.1 Skriptbasierte Services im GrantMA Self-Service-Portal bestellen

Hintergrund / Mehrwert

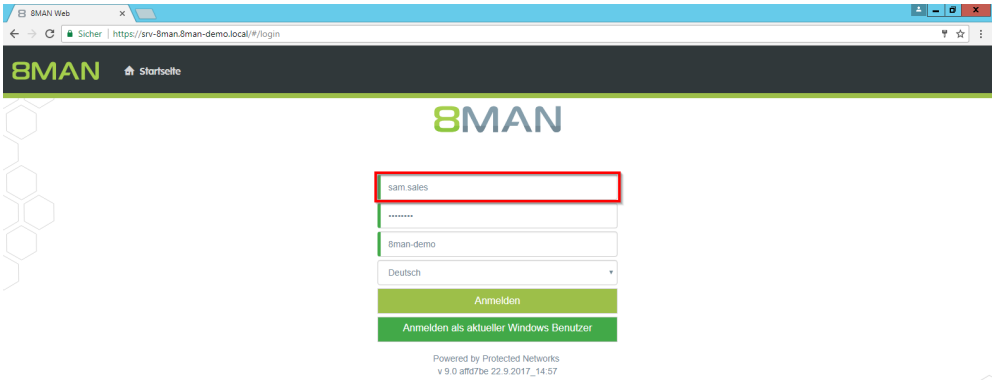
Neben der Bestellung von Nutzerkonten, Berechtigungen, Verzeichnissen oder frei definierbaren Objekten (Open Order) sind jetzt weitere skriptbasierte Services über den Webclient bestellbar.

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

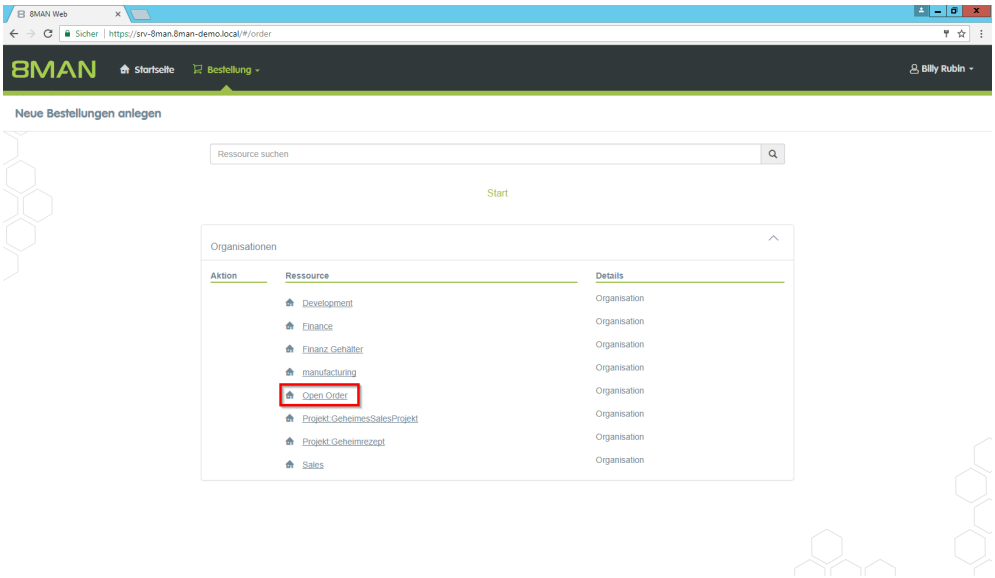
Einen skriptbasierten Service zur Bestellung konfigurieren (Administrator)

Der Prozess in einzelnen Schritten

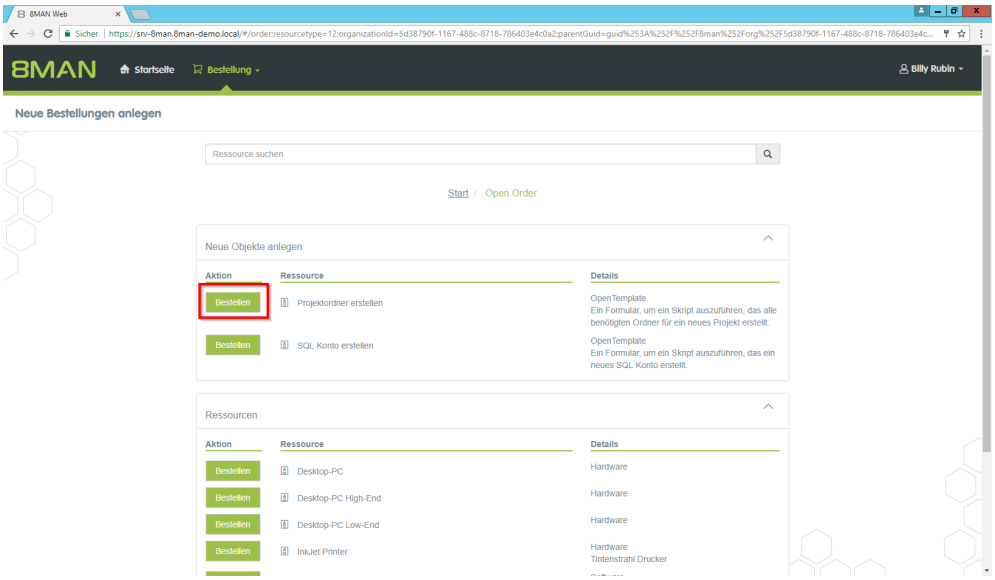


In dem folgenden Beispiel wird eine Projektordnerstruktur bestellt.

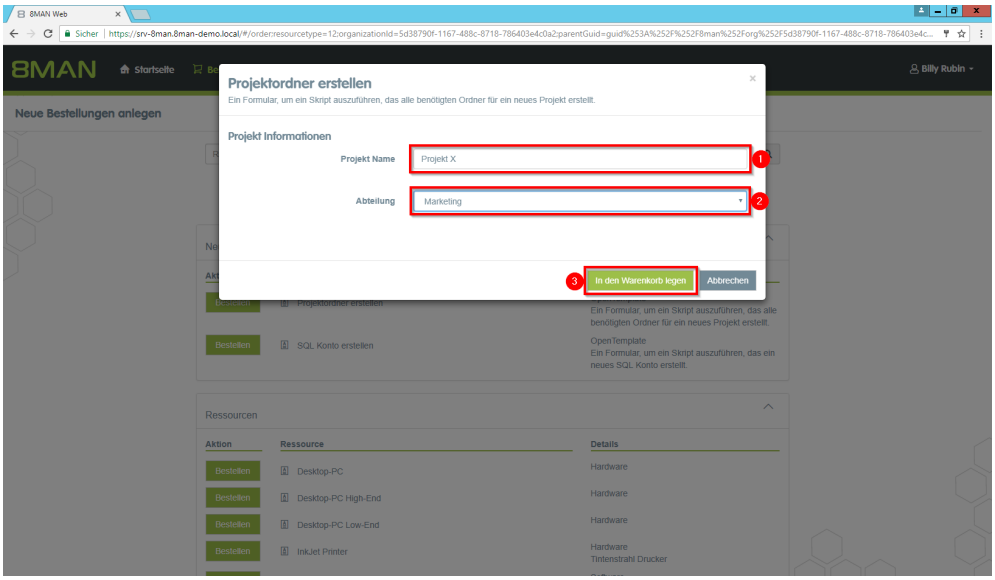
Loggen Sie sich als Besteller in den Webclient ein.



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

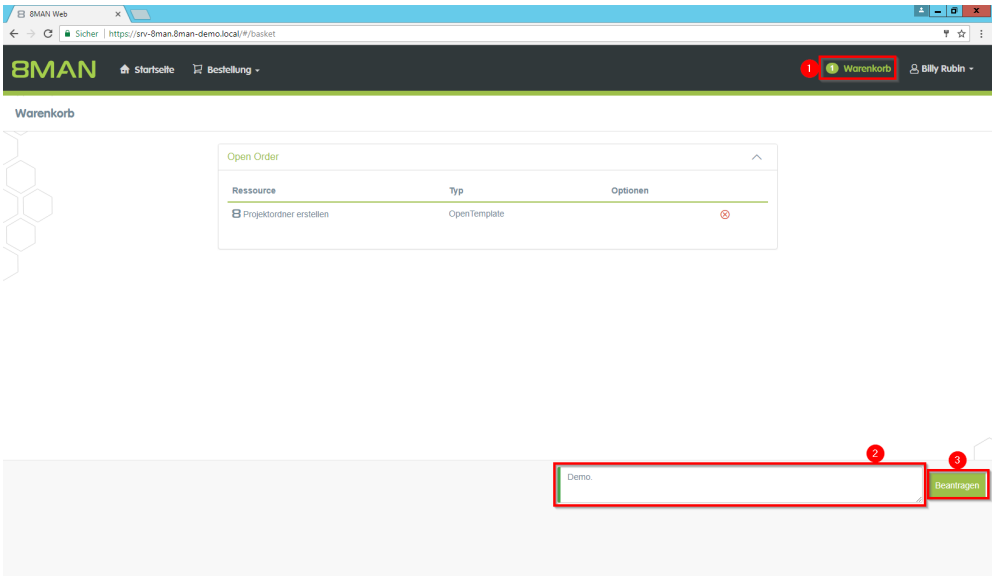


Wählen sie den Service "Projektordner erstellen" und klicken auf "Bestellen".



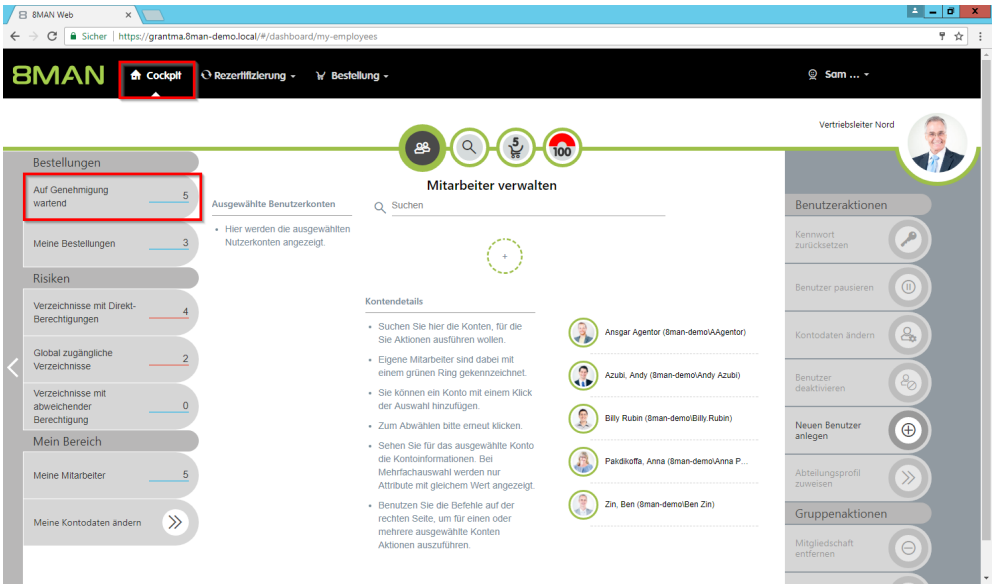
Geben Sie die Parameter zur Übergabe an das Skript ein. In dem Beispiel:

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:

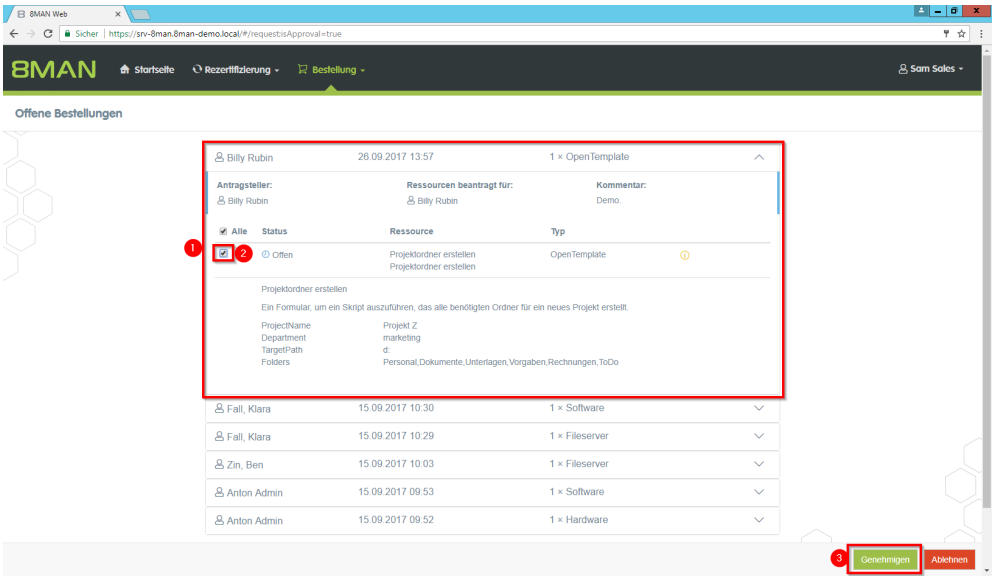
1. *Klicken Sie auf "Warenkorb".*
2. *Geben Sie einen Kommentar ein.*
3. *Klicken Sie auf "Beantragen".*



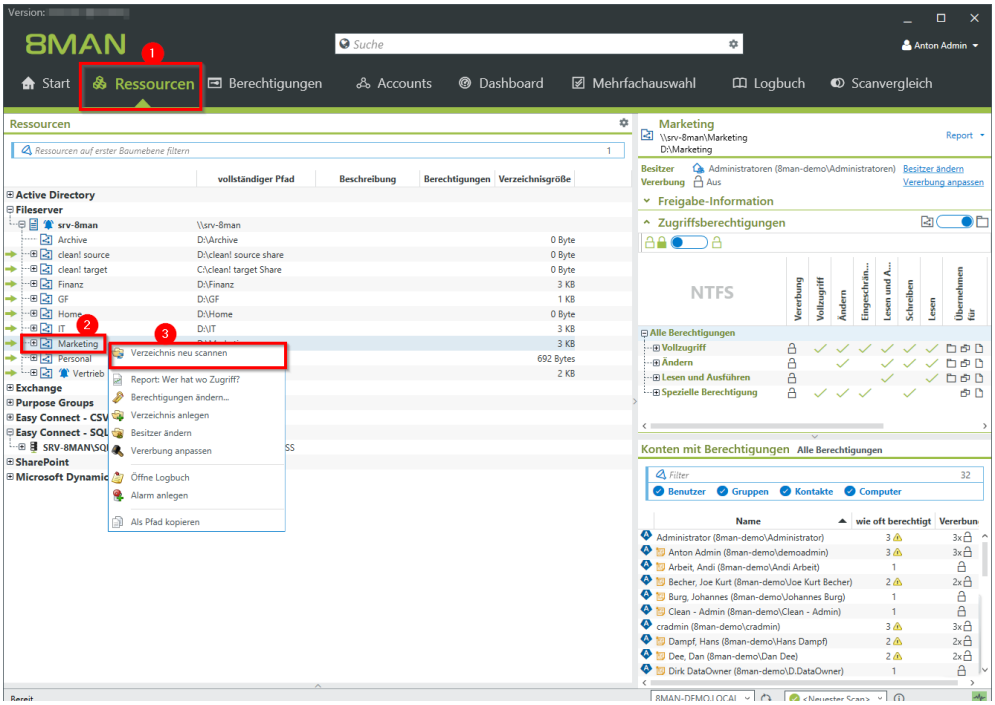
In dem hier gewählten Beispiel muss der Antrag durch Sam Sales genehmigt werden.

Melden Sie sich als Genehmiger an.

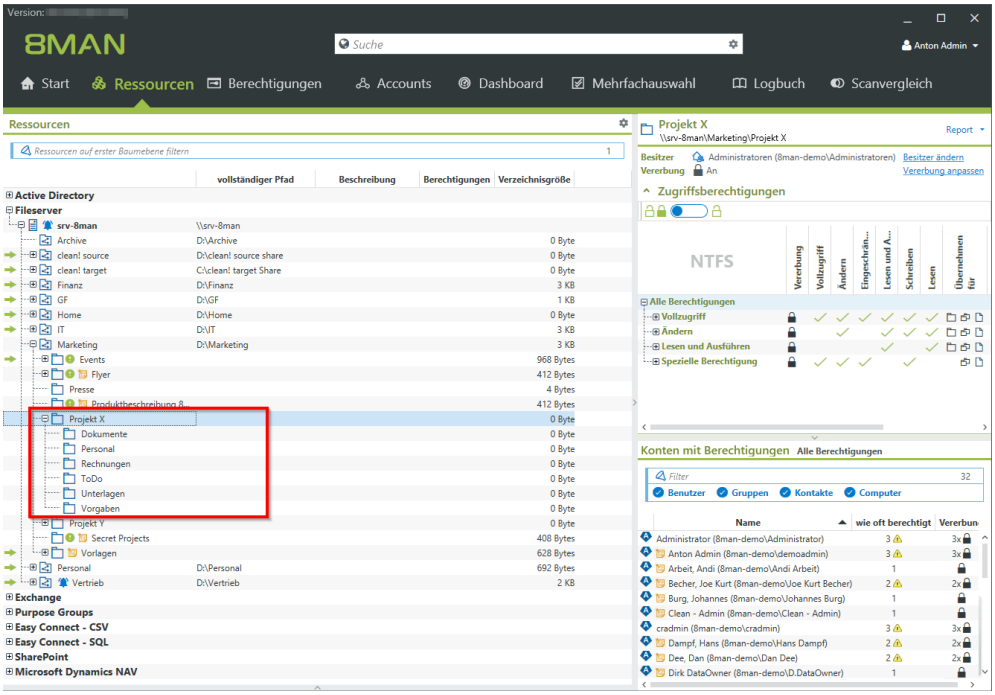
Klicken Sie auf "Auf Genehmigung wartend".



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.

5.2 Einen skriptbasierten Service zur Bestellung konfigurieren (Administrator)

Skriptbasierte Services stellen Sie im GrantMA Portal über Open (Order) Templates zur Verfügung.

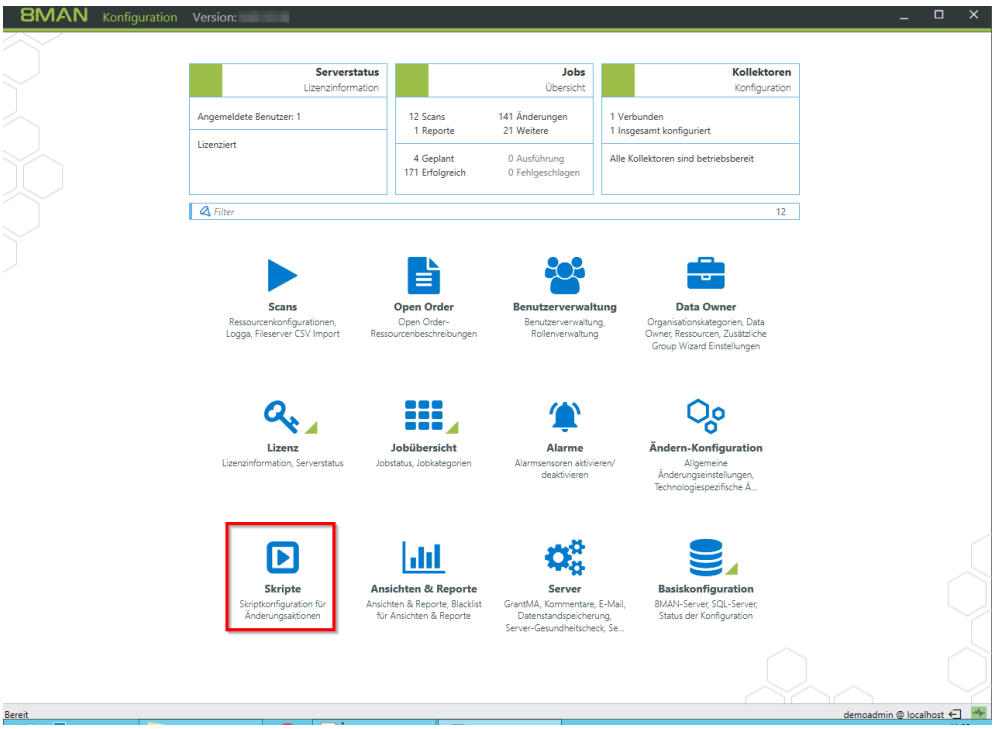
Wie Open Order Templates in 8MAN eingebunden werden, ist im Handbuch "Templates anpassen" beschrieben. Neu ab 8MAN Release 9 ist das Aufrufen eines Skriptes.

Beispiel

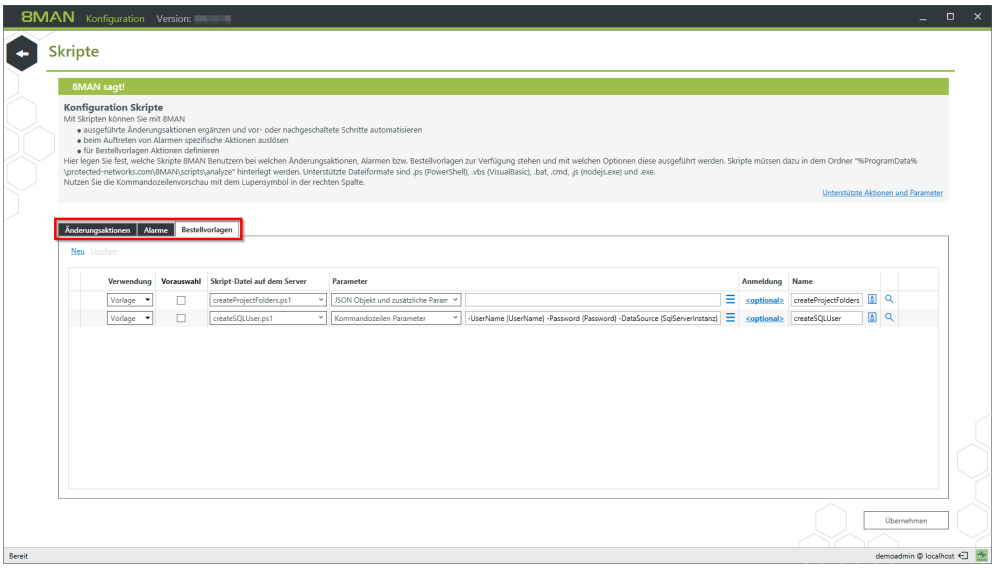
```
[
    {
        "Version": 1,
        "TemplateType": "OpenTemplate",
        "Id": "0E74ACA2-32A5-462C-A3A0-749A81D0B52A",
        "DisplayName": "Projektordner erstellen",
        "Description": "Ein Formular, um ein Skript auszuführen, das alle benötigten Ordner für ein
neues Projekt erstellt.",
             "IsManualInteractionRequired": false,
             "ScriptToExecute": "createProjectFolders",
        "Form": {
          "Type": "Container",
          "Label": "Projekt Informationen",
          "Templates": [
            { "Key": "ProjectName", "Value": {
                "Type": "TextField",
                "Label": "Projekt Name",
                           "IsRequired": true,
                           "Constraints": {
                                  "MaxLength": 248,
                                  "ForbiddenChars": [
                    "\"",
                    "\\",
                    "/",
                    ":",
                    "|",
                    "<",
                    ">",
                    "*",
                    "?"
                                  ]
                           }
                }
            },
            { "Key": "Department", "Value": {
                "Type": "DropDownList",
                "Label": "Abteilung",
                           "IsRequired": true,
                 "Items": [
                    {
                    "Value":"finanz",
                    "DisplayValue": "Finanz"
                    },
                    {
                    "Value": "gf",
                    "DisplayValue": "GF"
                    },
                    {
                    "Value": "it",
                    "DisplayValue": "IT"
                    },
                    {
                    "Value": "marketing",
                    "DisplayValue": "Marketing"
                    },
```

```
                {
                "Value": "personal",
                "DisplayValue": "Personal"
                },
                {
                "Value": "vertrieb",
                "DisplayValue": "Vertrieb"
                }
            ],
            "DefaultValue": ""
           }
        },
        { "Key": "TargetPath", "Value": {
            "Type": "TextField",
            "Label": "Target Path",
                        "IsHidden": true,
                        "DefaultValue": "d:"
            }
        },
        { "Key": "Folders", "Value": {
            "Type": "TextField",
            "Label": "Project folders",
                        "IsHidden": true,
                        "DefaultValue": "Personal,Dokumente,Unterlagen,Vorgaben,Rechnungen,ToDo"
            }
        }
      ]
    }
  }
]
```

Die Skripte müssen in der 8MAN Konfiguration bereitgestellt werden. Dies erfolgt analog zu den Skripten, die nach Änderungen in 8MAN ausgeführt werden.



Ab Version 9 können Skripte nicht nur nach Änderungen, sondern auch nach Alarmen oder in Open Order Templates aufgerufen werden. Deshalb ist der Menüpunkt Skripte nun direkt auf der Startseite der 8MAN Konfiguration (und nicht mehr unter Ändern-Konfiguration).



Die Skriptkonfiguration ist in 3 Tabs unterteilt: "Änderungsaktionen", "Alarme" und "Bestellvorlagen".

5.3 Rezertifizierung

5.3.1 Zu rezertifizierende Ressourcen festlegen

Vor der Version 9 wurde die Rezertifizierung global für Ressourcen aktiviert, die folgenden Bedingungen erfüllten:

- Ressource ist vom Typ Fileserver
- Ressource hat einen DataOwner zugeordnet
- Ressource ist als änderbar gesetzt

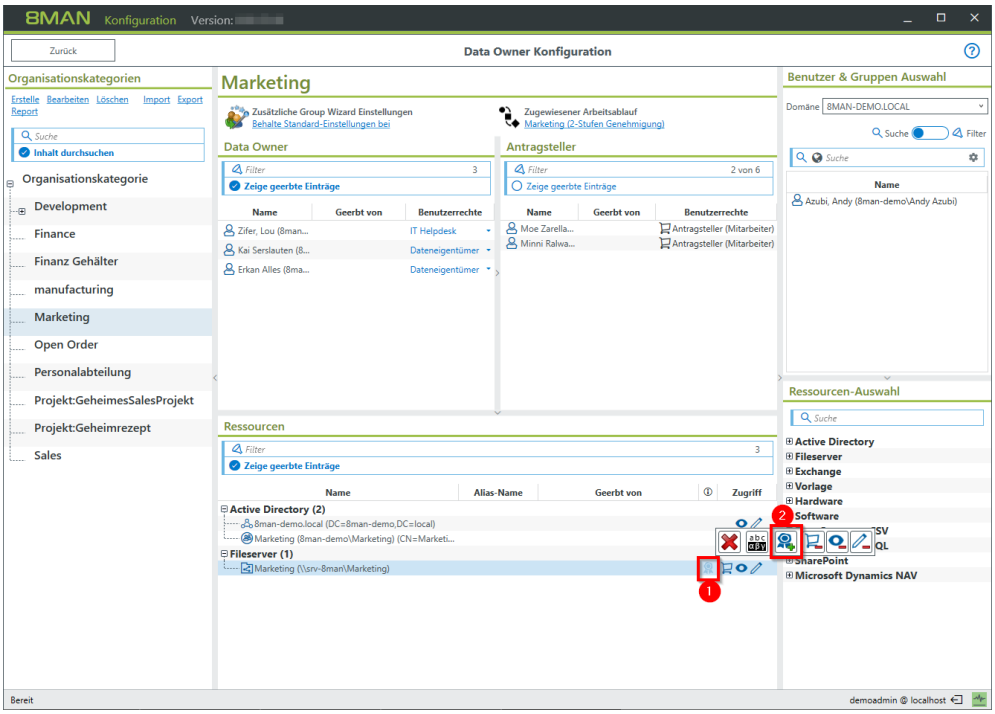
Ab der Version 9 setzen Sie in der DataOwner-Konfiguration separat für die Fileserver-Ressourcen, ob diese rezertifiziert werden müssen.

8MAN Verhalten bei bestehender DataOwner-Konfiguration

Alle bereits zugeordneten Fileserver-Ressourcen erfordern wie bisher eine Rezertifizierung. Diese kann nun je Zuordnung separat deaktiviert werden.

8MAN Verhalten bei Ersteinrichtung der DataOwner-Konfiguration

Die Rezertifizierung ist standardmäßig deaktiviert und muss je zugeordneter Ressource aktiviert werden.



1. *Das "Siegel"-Symbol zeigt an, ob die Rezertifizierung für die Ressource aktiviert ist.*
2. *Aktivieren/Deaktivieren Sie die Rezertifizierung für die selektierte Ressource.*

5.3.2 Benachrichtigungs-E-Mails für die Rezertifizierung testen

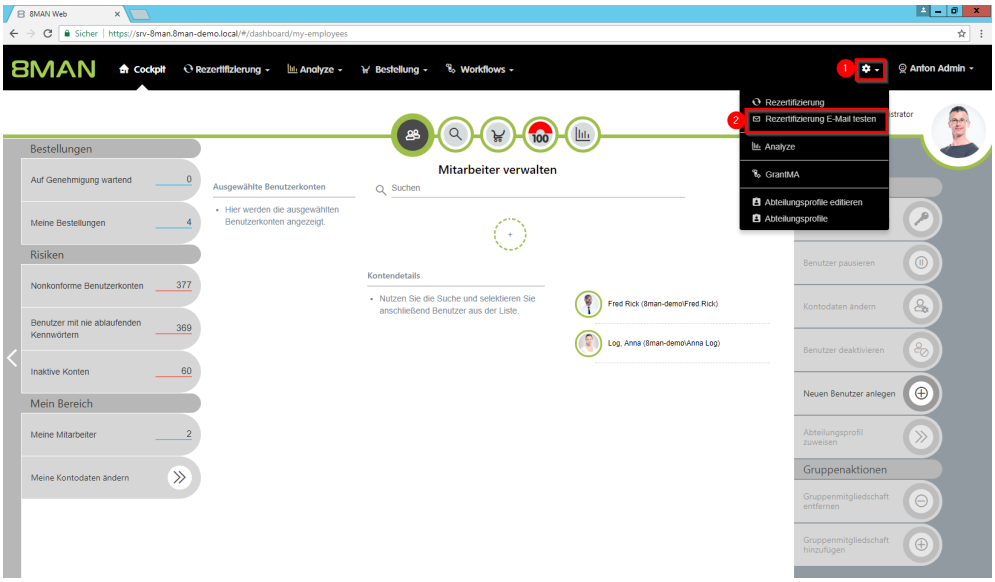
Hintergrund / Mehrwert

In den Stadien der Rezertifizierung versendet 8MAN diverse Benachrichtigungs-E-Mails. Testen Sie die Benachrichtigungs-E-Mails - auch ggf. Ihre Anpassungen, bevor Sie die Rezertifizierung aktivieren.

Weiterführende Services

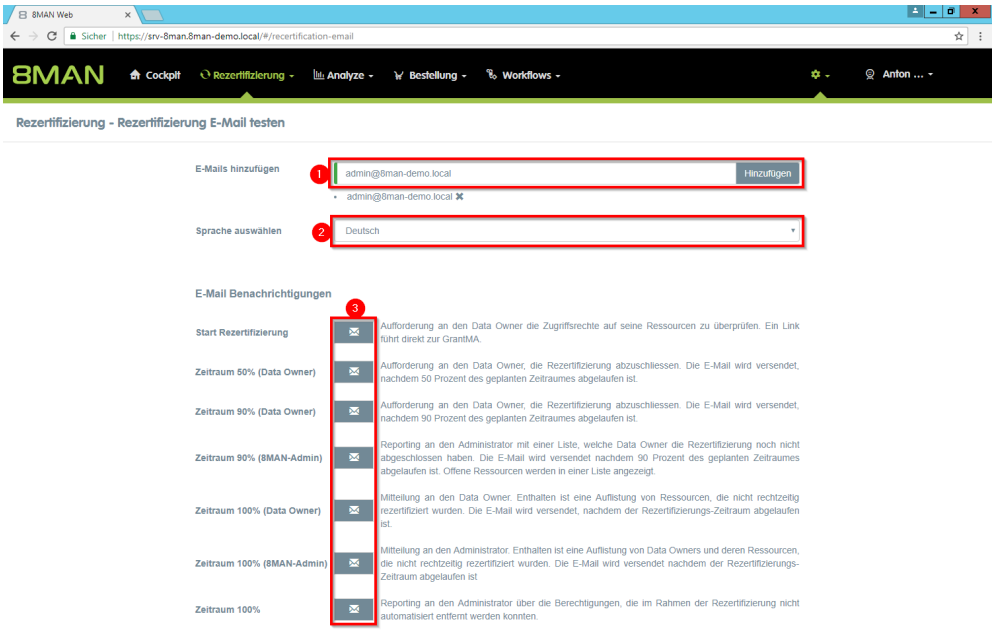
Benachrichtigungs-E-Mails für die Rezertifizierung anpassen (Administrator)

Der Prozess in einzelnen Schritten



Loggen Sie sich als Administrator in den Webclient ein.

1. *Klicken Sie auf das Zahnrad.*
2. *Wählen Sie "Rezertifizierung E-Mail testen".*



1. *Geben Sie eine oder mehrere Empfänger an.*
2. *Wählen Sie die Sprache.*
3. *Versenden Sie die gewünschte Benachrichtigungs-E-Mail.*

Beispiel für eine Benachrichtigung zum Start der Rezertifizierung.

Rezertifizierung

Sehr geehrte(r) Anton Admin,

eine turnusmäßige Rezertifizierung steht an. Diese muss spätestens bis zum 17.01.2018 abgeschlossen sein.
Überprüfen Sie die Berechtigungen auf folgenden Ressourcen:

Berechtigungen

Ressource	Beschreibung
ProjectX	Project X
ProjectY	Project Y

Benutzen Sie diesen Link, um sich auf der 8MAN Rezertifizierungswebsite einzuloggen.

Mit freundlichen Grüßen

8MAN Rezertifizierung

6 User Provisioning

6.1 Abteilungsprofile definieren, anwenden und prüfen (Compliance Check)

8MAN setzt im Bereich User Provisioning neue Maßstäbe: Mit der Einführung von Nutzerprofilen 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:

Wird ein Nutzerkonto angelegt, erhält es das für den Aufgabenbereich definierte Profil. Wechselt der Mitarbeiter die Abteilung, kann der Vorgesetzte einfach sein Abteilungsprofil auf das entsprechende Nutzerkonto anwenden.

Erhält der Mitarbeiter weitere Berechtigungen, die vom Standard abweichen, zeigt ein Compliance-Monitor dem Vorgesetzten die Abweichungen. In Form von Bulk-Operationen, kann der Abteilungsleiter die Nutzerkonten entsprechend der Profile in seiner Abteilung harmonisieren. Dies ist vor allem dann wichtig, wenn das Abteilungsprofil aktualisiert wurde.

Services

Ein neues Abteilungsprofil erstellen (Administrator)

Benutzern ein Abteilungsprofil zuweisen (Cockpit)

Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check)

6.1.1 Ein neues Abteilungsprofil erstellen (Administrator)

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:

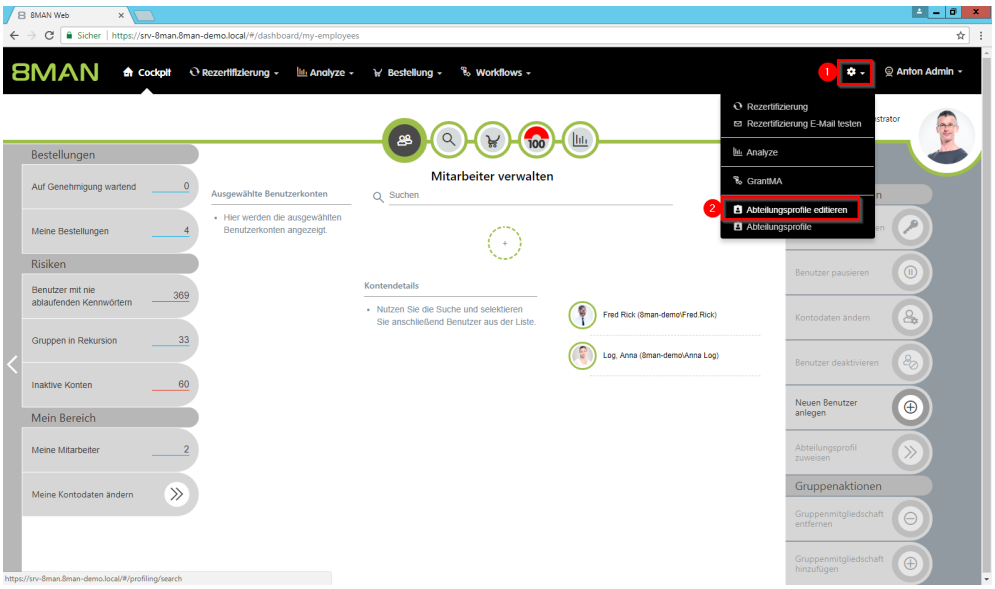
Abteilungsprofile können Attribute und Gruppenmitgliedschaften enthalten.

Weiterführende Services

Benutzern ein Abteilungsprofil zuweisen (Webclient)

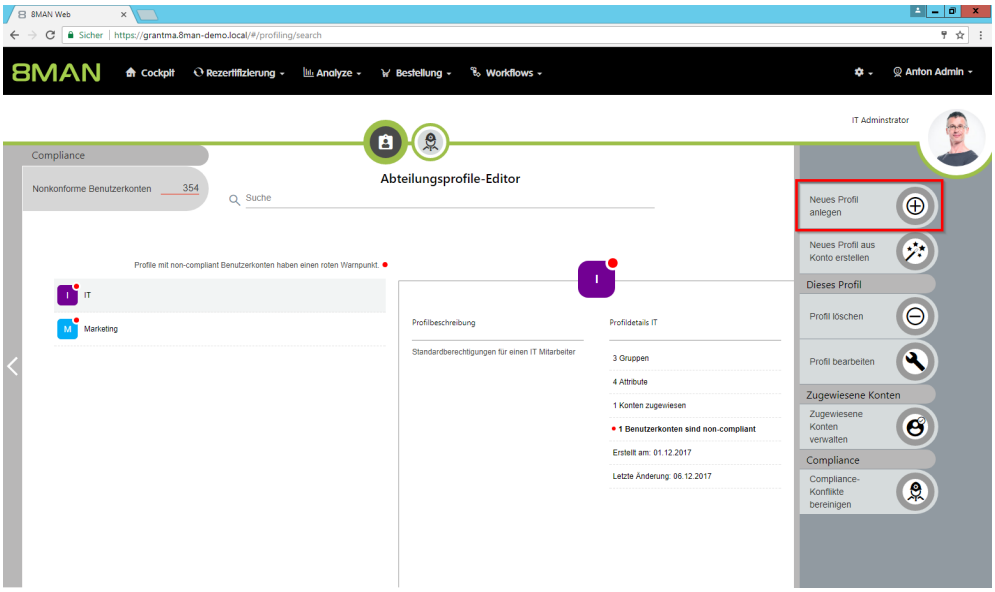
Vom Abteilungsprofil abweichende Berechtigungen ermitteln (Compliance Check) (Webclient)

Der Prozess in einzelnen Schritten

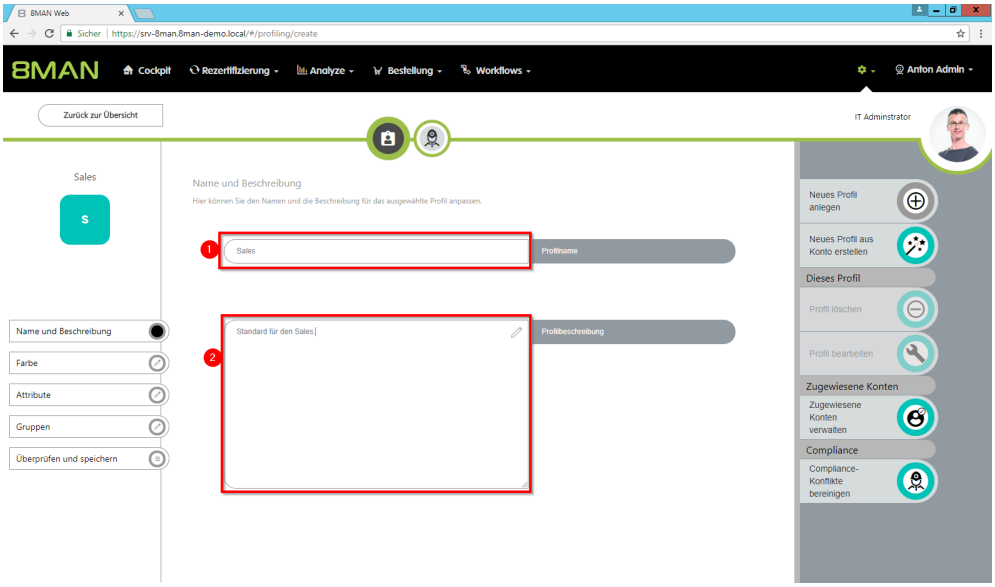


Klicken Sie auf "Abteilungsprofile editieren".

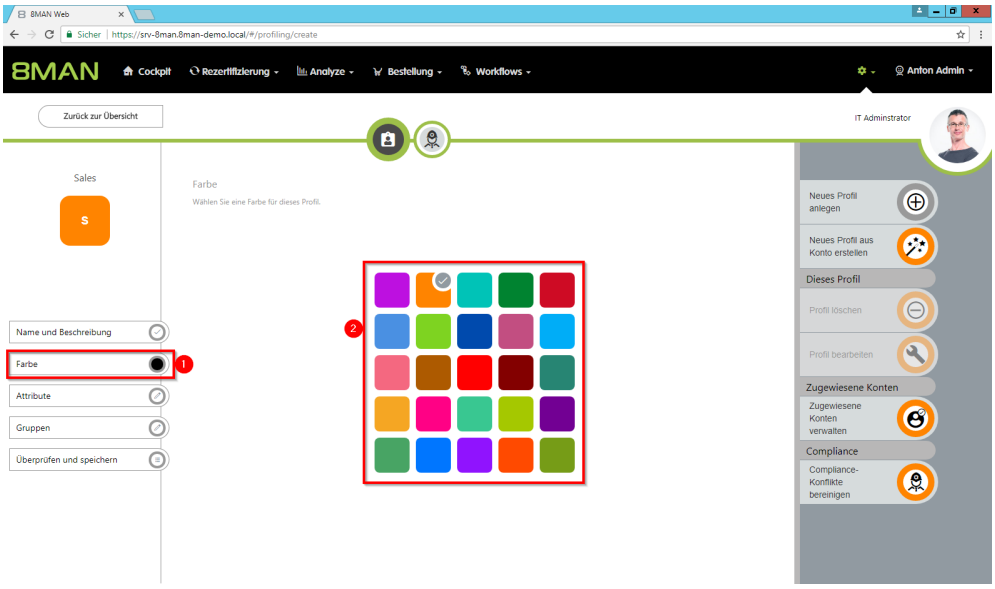
Sie müssen als 8MAN Administrator eingeloggt sein, um das Zahnradsymbol sehen zu können.



Klicken Sie auf "Neues Profil anlegen".

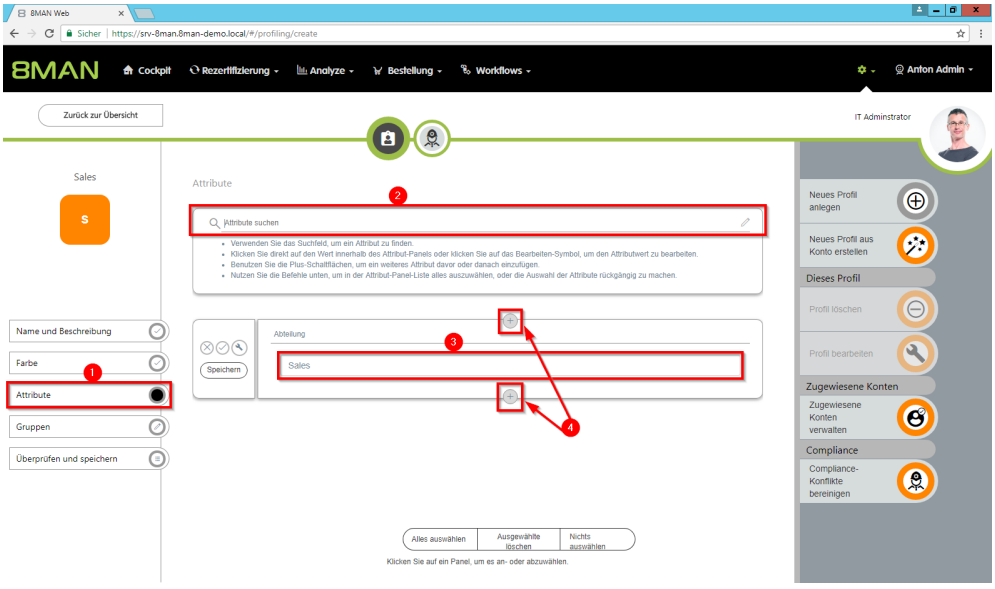


1. *Geben Sie dem Abteilungsprofil einen Namen, mindestens 3 Buchstaben.*
2. *Optional: Beschreiben Sie das Profil.*

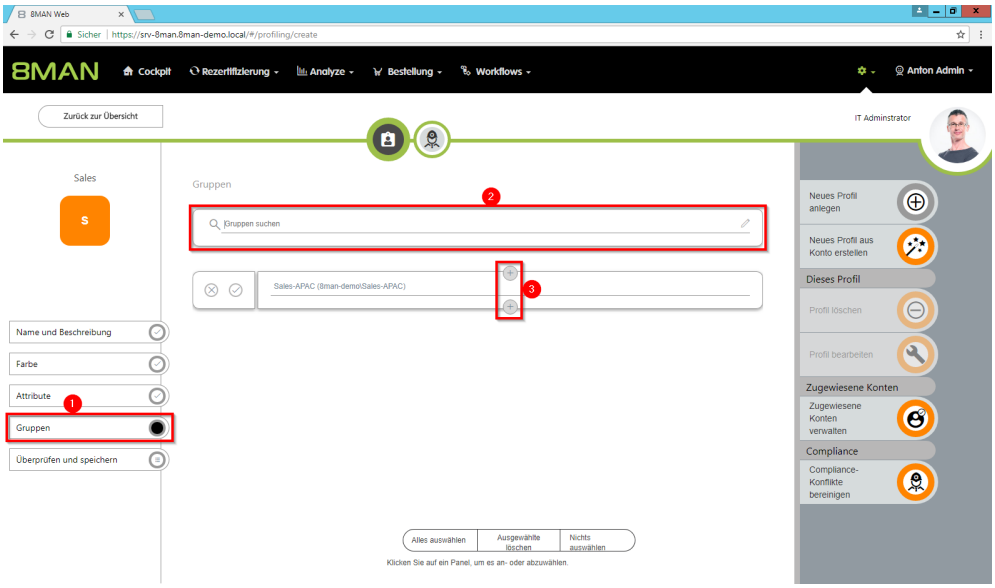


1. *Klicken Sie auf "Farbe".*
2. *Wählen Sie eine Farbe für das Abteilungsprofil.*

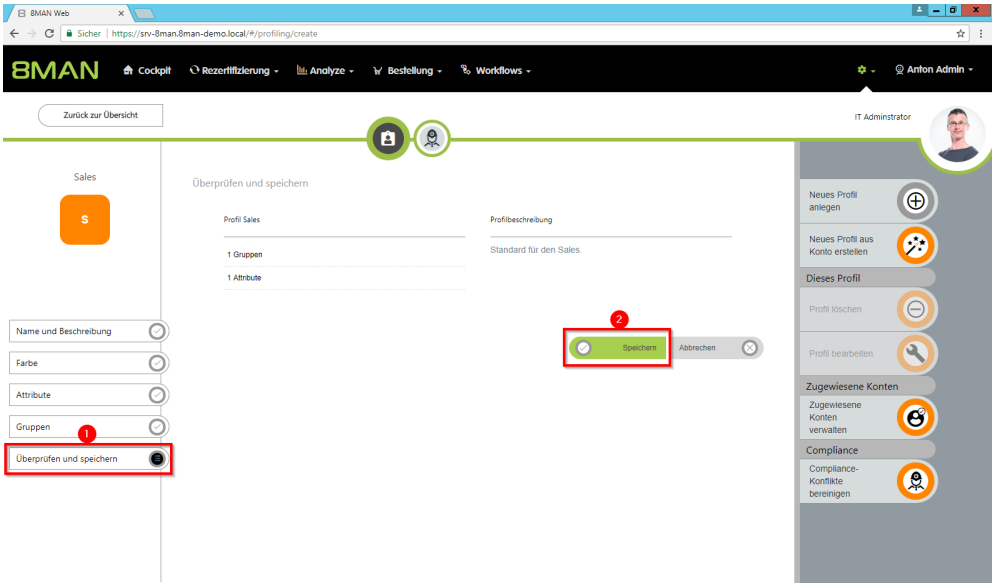
Die Farbe dient der Wiedererkennung.



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.*

6.2 Computerkonten editieren

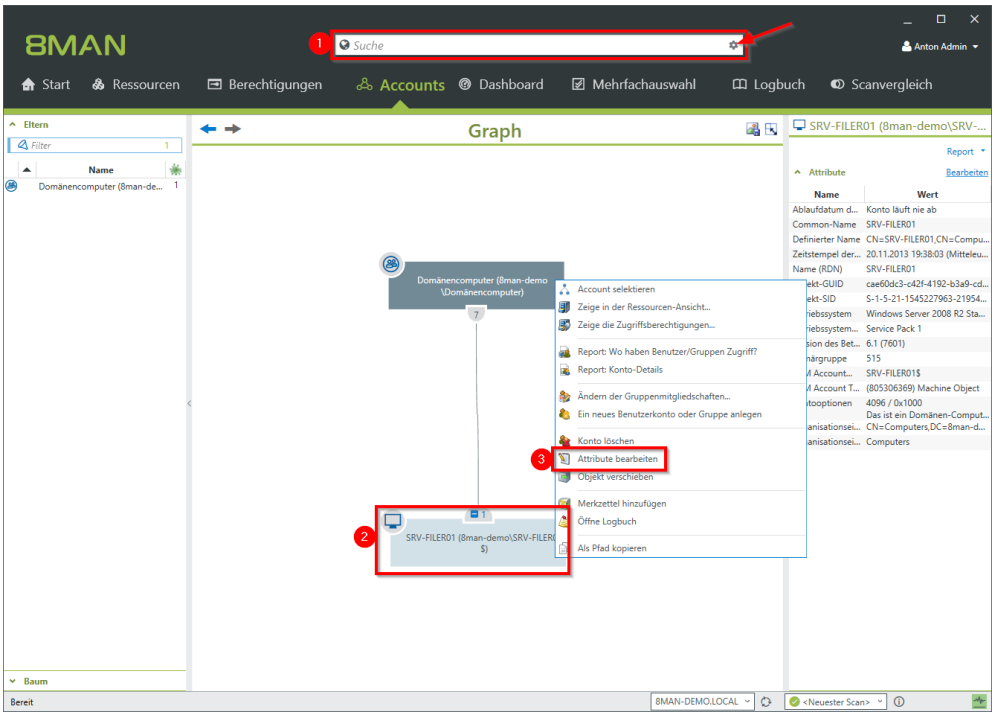
Hintergrund / Mehrwert

Pflegen Sie Computerkonten komfortabel und dokumentiert innerhalb 8MAN.

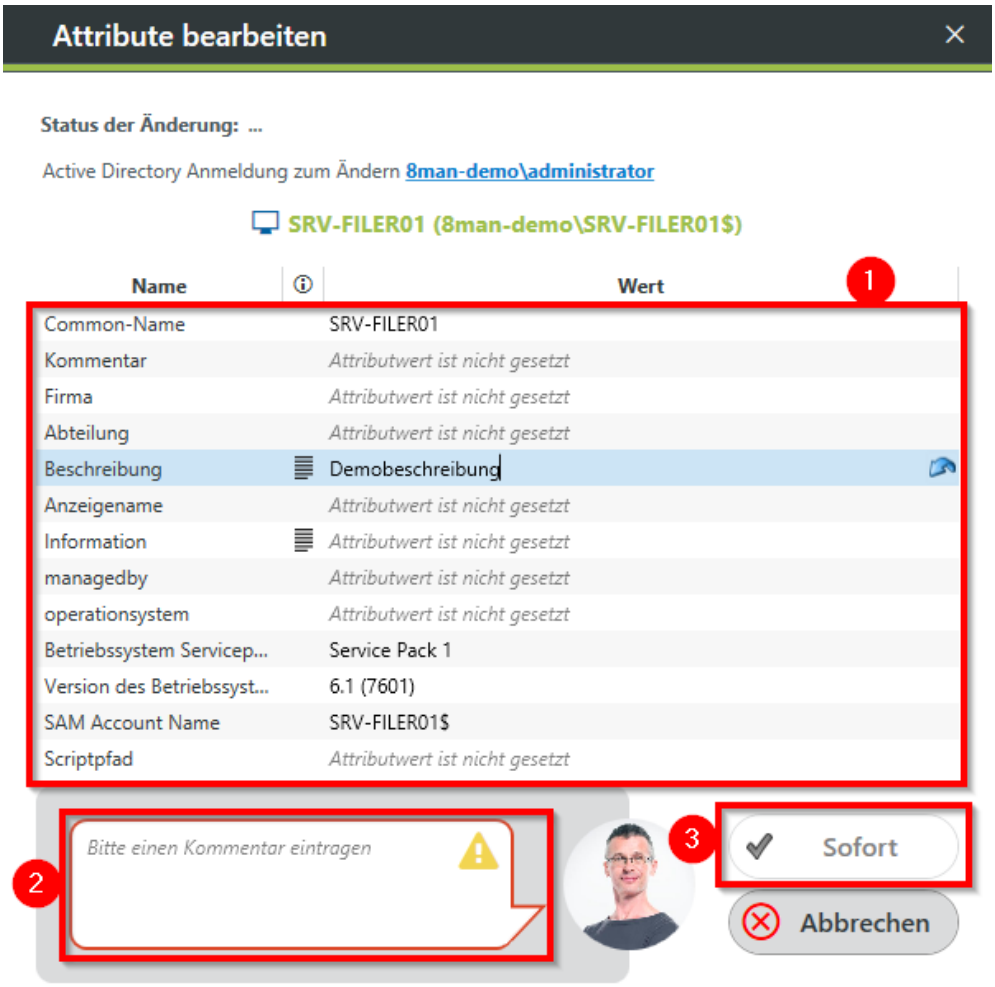
Weiterführende Services

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.*

6.3 Computerkonten löschen

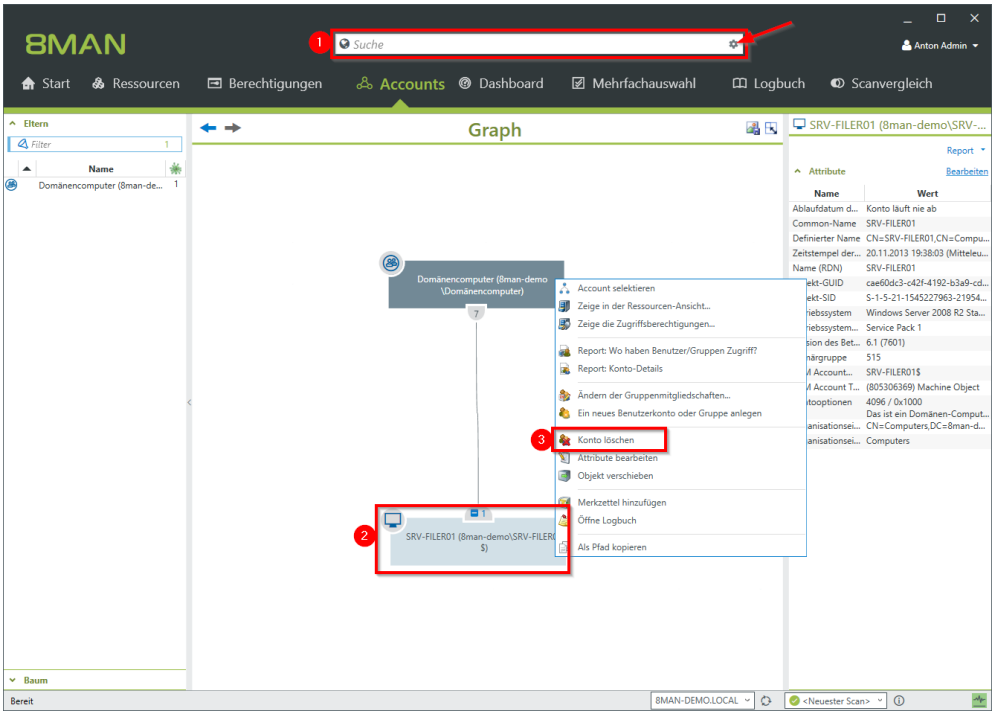
Hintergrund / Mehrwert

Löschen Sie Computerkonten komfortabel und dokumentiert innerhalb 8MAN.

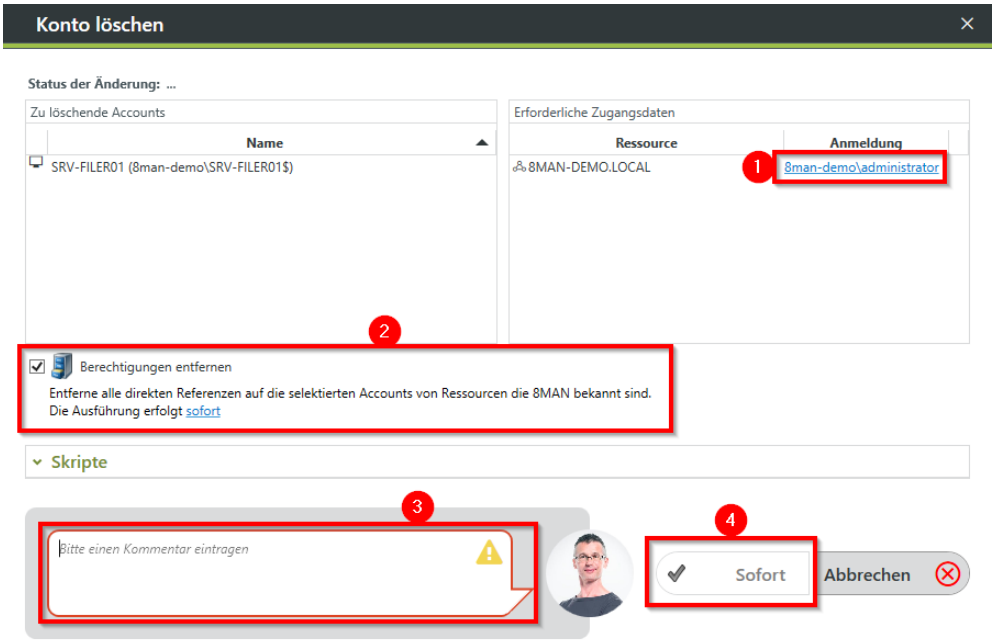
Weiterführende Services

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.*

7 Resource Integration

7.1 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.

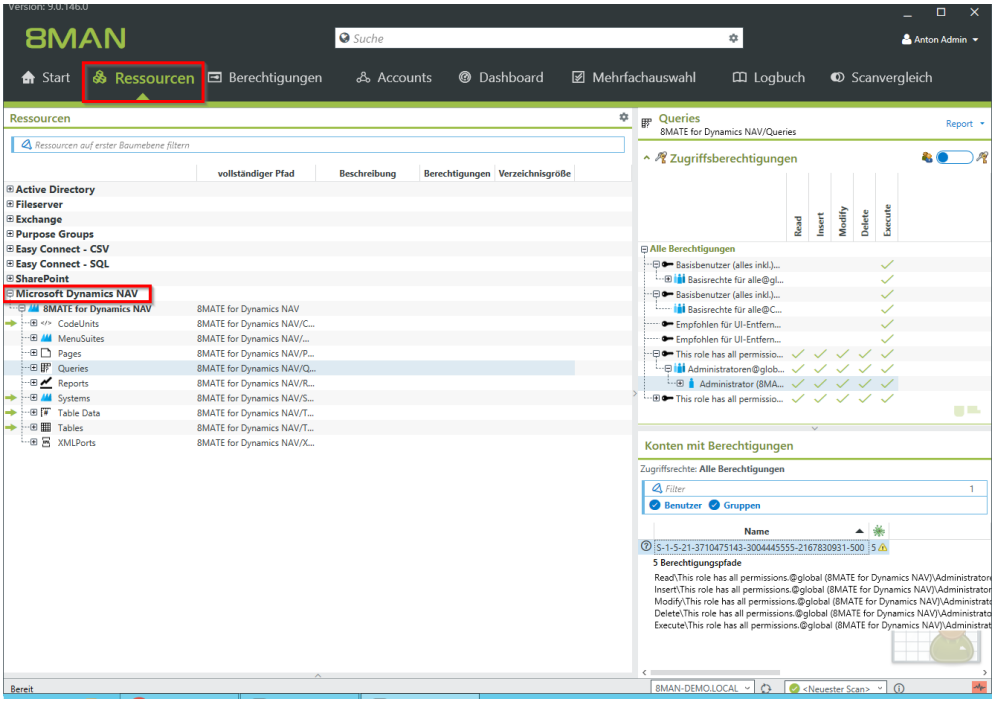
Das 8Mate Dynamics NAV integriert die Berechtigungsanalyse des ERP-Systems in 8MAN. In gewohnter Weise sehen Sie alle Zugriffsrechte in einer flachen Liste. Im ersten Schritt bietet das Modul Services im Bereich Permission Analysis und Documentation & Reporting:

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.

8 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.

Urheberrecht

Protected Networks GmbH
Alt-Moabit 73
10555 Berlin

+49 30 390 63 45 - 0
www.protected-networks.com
www.8man.com

9 Software-Lizenzvereinbarungen

- 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
- 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

A

C