8MAN

Access Rights Management. Only much Smarter.

Access Rights Management

AD Logga Handbuch

Version 9

Protected Networks

1 Security Monitoring

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

Auf Prozessebene erlangen Sie vollständige Transparenz über die Access Rights Aktivitäten. Selbst außerhalb von 8MAN vorgenommene Änderungen werden erfasst. Auf Basis der gewonnenen Informationen lässt sich Ihr Access Rights Management Prozess optimieren.

Mit den enthaltenen Alerts werden Sie bei kritischen Ereignissen in Echtzeit, proaktiv informiert.

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

Active Directory

8MATE AD Logga

Fileserver

8MATE FS Logga

1.1 8MATE AD Logga

Problem

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

Sicherheitsrisiken

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

Unklare Prozesse

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

Lösung

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

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

Das erreichen Sie mit dem AD Logga

- Administratoren erhalten ein vollständiges Bild über die Aktivitäten im AD. Prozesse können so optimiert werden.
- Auditoren erkennen Sicherheitsvorfälle und die involvierten Akteure. Maßnahmen können so ergriffen werden.
- Die Geschäftsführung hat die Gewissheit: Der AD Logga stellt mit seinem Monitoring die Daten für interne Sicherheit und Prozessverbesserungen bereit.

Mit dem 8MATE AD Logga überwachen Sie permanent Änderungen am AD. Der AD Logga erfasst auch Änderungen, die nicht mit 8MAN ausgeführt wurden.

Die folgenden Änderungen werden vom AD Logga überwacht:

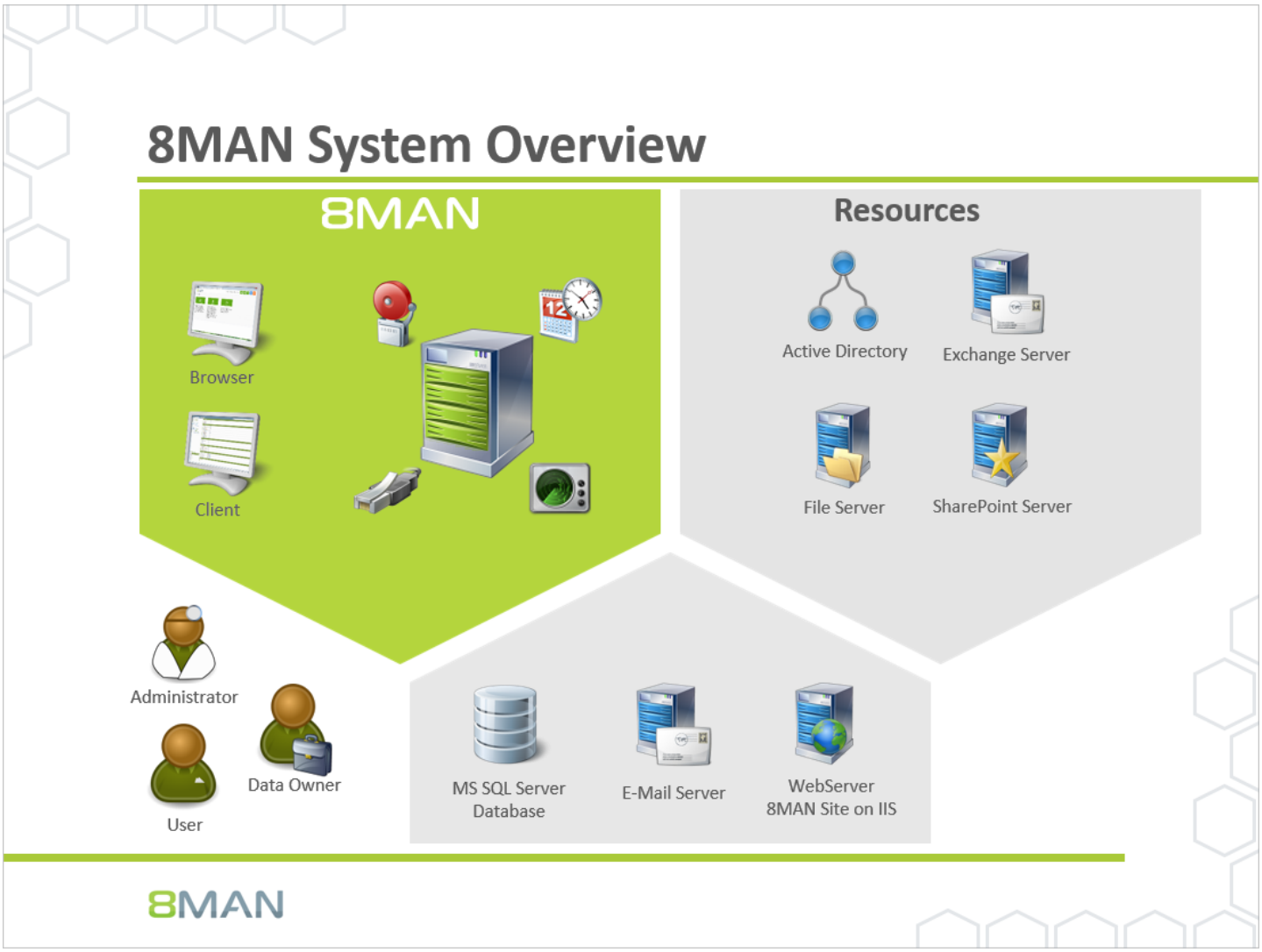
- AD Objekt erzeugt / gelöscht
- AD Objekt verschoben
- Gruppe, Benutzer- oder Computerkonto erstellt / gelöscht
- Gruppenmitgliedschaft geändert
- Konto aktiviert / deaktiviert
- Kennwort zurückgesetzt
- Konto gesperrt / entsperrt
- Attribut-Änderungen von AD Objekten (z. B. Gruppentyp, Distinguished Name, Department …)

Erfasste Änderungen werden in der 8MAN Datenbank abgelegt und sind über das 8MAN Logbuch und Reporte kategorisiert abrufbar.
Der 8MAN AD Logga arbeitet agentenlos. Sie müssen also keine extra Software auf den Domänencontrollern installieren. Unterstützte Server Versionen sind in den Systemvoraussetzungen beschrieben.

Die vom 8MATE AD Logga verwendete Technologie stellt sicher, dass alle Ereignisse lückenlos aufgezeichnet werden. Kurzfristige Ausfälle des 8MAN Kollektors, z.B. wegen Wartung, führen nicht zu fehlenden Ereignissen im 8MAN Logbuch.

2 Systemvoraussetzungen

2.1 Die 8MAN Architektur



Die 8MAN Suite gliedert sich in drei Komponenten:

- 8MAN Server für die Verarbeitung der neuen Daten sowie der Anfragen von der grafischen 8MAN Benutzeroberfläche
- Kollektoren zur Anbindung der Ressourcensysteme und Datenverarbeitung
- 8MAN Benutzeroberflächen (Anwendungs- und Konfigurationsoberfläche, Weboberfläche)

Das Komponentenmodell der 8MAN Suite erlaubt es, Remote-Ressourcen durch verteilte Installationen optimal zu unterstützen. Alle Komponenten sind untereinander über netzwerkfähige Schnittstellen verbunden. Es können auch mehrere Komponenten auf dem gleichen Computer betrieben werden.

2.2 AD Logga Voraussetzungen

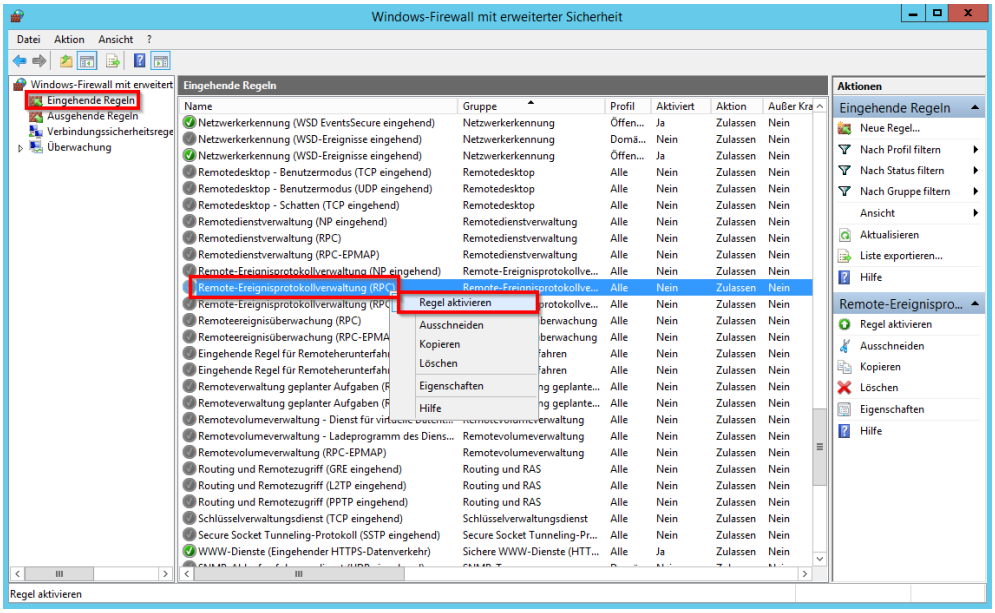
Der 8MATE AD Logga unterstützt Domänen Controller (DCs), die unter folgenden Server Versionen laufen:

- Microsoft Windows Server 2008 (32-bit und 64-bit), 2008 R2, 2012, 2012 R2 und 2016

Für den 8MATE AD Logga ist kein dedizierter Kollektor erforderlich. Der 8MAN Server selbst kann z. B. als Kollektor verwendet werden.

2.3 Netzwerkanforderungen und Firewall-Einstellungen

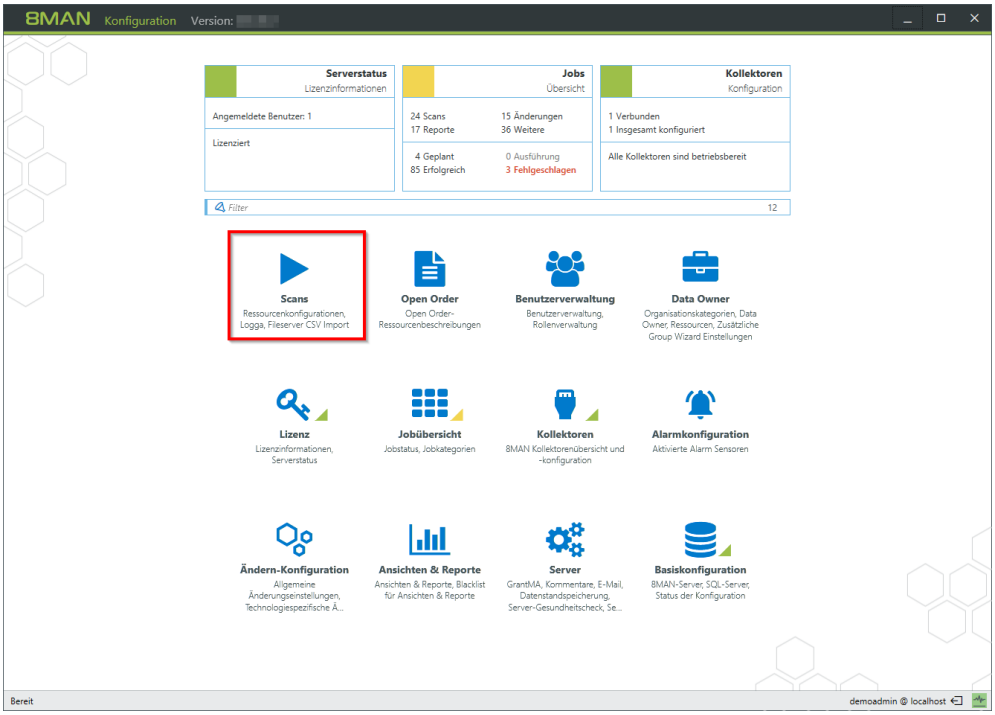
2.3.1 Die Windows Firewall für den AD Logga einrichten



Ist die Windows Firewall auf dem zu überwachenden DC eingeschaltet, müssen Sie die von Microsoft vordefinierte Regel "Remote-Ereignisprotokollverwaltung (RPC)" aktivieren.

Wiederholen Sie den Vorgang für jeden zu überwachenden DC.

3 Scans und Logga konfigurieren



8MAN scannt in konfigurierbaren Intervallen Berechtigungsstrukturen von verschiedenen Ressourcen-Systemen. Die Scan-Ergebnisse speichert 8MAN in einer SQL-Datenbank. Benutzer sehen in der Benutzeroberfläche sehr schnell die Ergebnisse, weil diese aus der Datenbank abgerufen werden.

Ereignisse, die zwischen den Scans passieren, erfassen die 8MATES AD Logga und FS Logga. 8MATES sind Add-Ons zu den Basisversionen von 8MAN und benötigen eine entsprechende Lizenz.

Klicken Sie auf "Scans", um Ressourcen-Scans und die Logga zu konfigurieren.

3.1 Active Directory (AD) Logga konfigurieren

3.1.1 Überwachung für den AD Logga aktivieren

3.1.1.1 Überwachungsrichtlinien für die Domänencontroller (DC) konfigurieren

Für die AD Logga Funktionalität müssen Sie spezielle Überwachungsrichtlinien (Audit Policies) aktivieren.
Um Überwachungsrichtlinien auf DCs ändern zu können, müssen Sie Mitglied der entsprechenden Domänen-Admins Gruppe oder der Gruppe der Organisations-Admins sein.

3.1.1.1.1 Überwachungsrichtlinien für DCs in Server 2008 konfigurieren

Führen Sie vor dem Setzen der Überwachungsrichtlinien eine Prüfung aus - ggf. sind ja bereits alle erforderlichen Kategorien aktiviert.
Für die Aktivierung der erforderlichen Überwachungsrichtlinien führen Sie folgende Kommandos auf jedem DC mit Administratorrechten aus:

Für „Richtlinienänderungen überwachen“:

```
auditpol /set /subcategory:{0CCE922F-69AE-11D9-BED3-505054503030} /success:enable
```

Für „Verzeichnisdienständerungen“:

```
auditpol /set /subcategory:{0CCE923C-69AE-11D9-BED3-505054503030} /success:enable
```

Für „Benutzerkontenverwaltung“, „Computerkontoverwaltung“, „ Sicherheitsgruppenverwaltung“, „Verteilergruppenverwaltung“, „Anwendungsgruppenverwaltung“ und „Andere Kontoverwaltungsereignisse“:

```
auditpol /set /subcategory:{0CCE9235-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9236-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9237-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9239-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE923A-69AE-11D9-BED3-505054503030} /success:enable
```

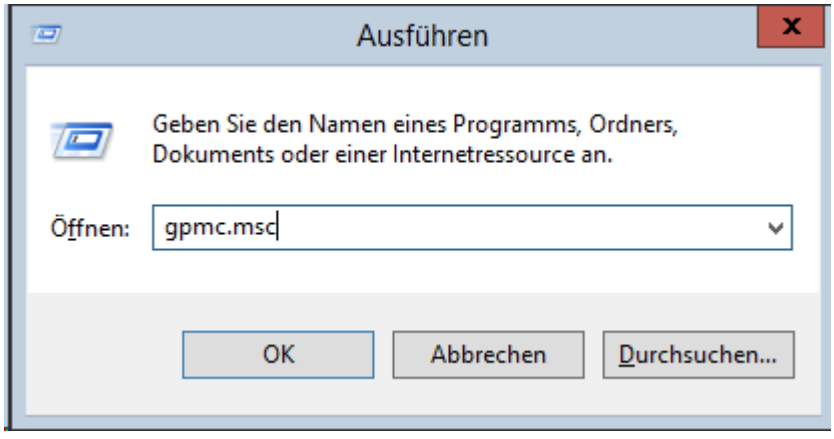
Wiederholen Sie den Vorgang für jeden DC!

3.1.1.1.2 Überwachungsrichtlinien für DCs ab Server 2008 R2 konfigurieren

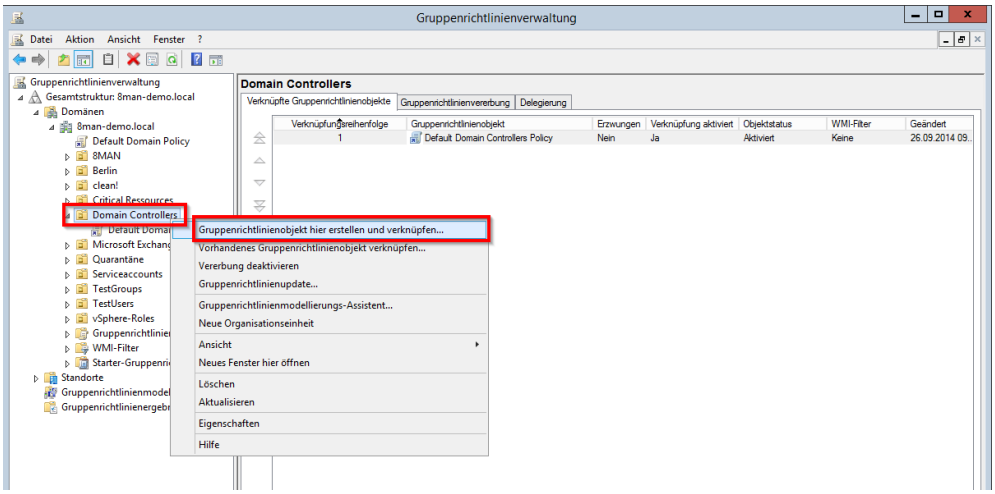
Ab Server 2008 R2 können Sie den Gruppenrichtlinien-Editor zur Einrichtung der Überwachung benutzen. Damit müssen Sie die Einrichtung nur einmal vornehmen und nicht mehr auf jedem DC wiederholen.
Beachten Sie dabei, dass sich die Aktivierung der Überwachungsrichtlinien je nach Replikationsintervall zwischen den Domänencontrollern (DCs) verzögert.

Nachdem Sie die folgenden Einstellungen vorgenommen haben:

- führen Sie ein manuelles Richtlinienupdate mit dem Kommando "gpupdate /force" aus,
- prüfen Sie die Ausführung der Überwachungsrichtlinien.



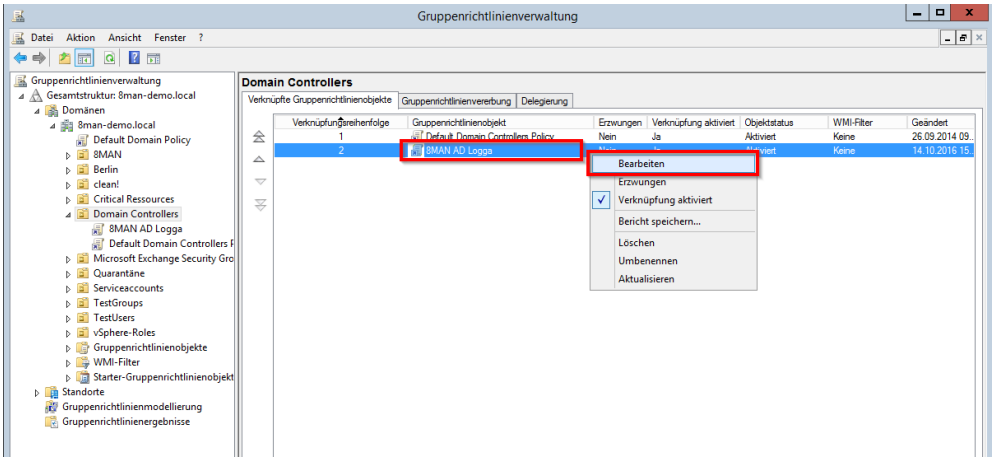
Starten Sie die Gruppenrichtlinienverwaltung, z. B. mit:
gpmc.msc



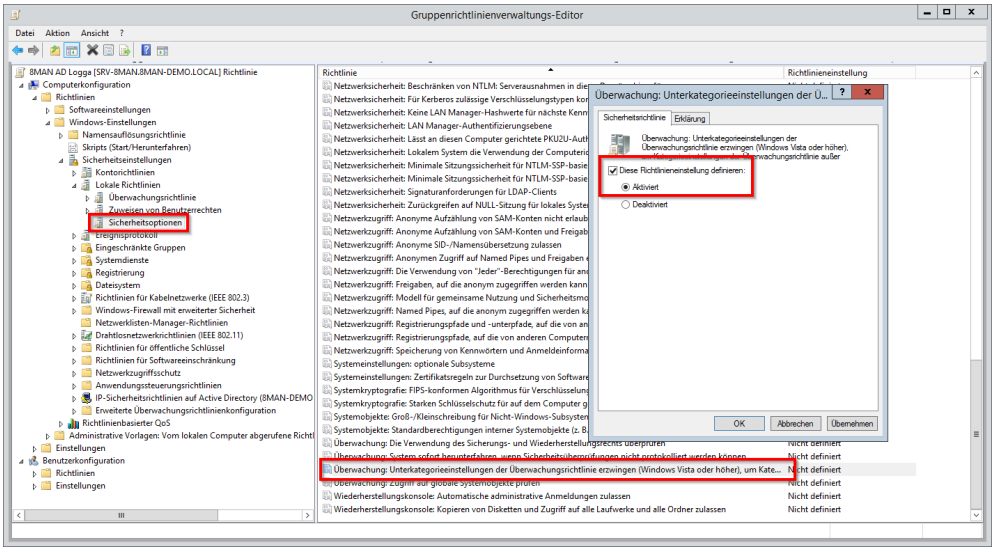
Erstellen Sie eine neue Gruppenrichtlinie. Wählen Sie die OU, in der die DC Computerkonten sind, standardmäßig ist das die OU "Domain Controllers".

Stellen Sie sicher, dass die neu erstellte Richtline für die DCs wirksam ist (Hierarchie, Abarbeitungsreihenfolge).

Die Reihenfolge, in der Sie die Optionen setzen, beeinflusst die Wirksamkeit der Richtlinie. Halten Sie die hier vorgegebene Reihenfolge ein!



Wählen Sie die neu erstellte Gruppenrichtlinie mit Rechtsklick und dann "Bearbeiten".

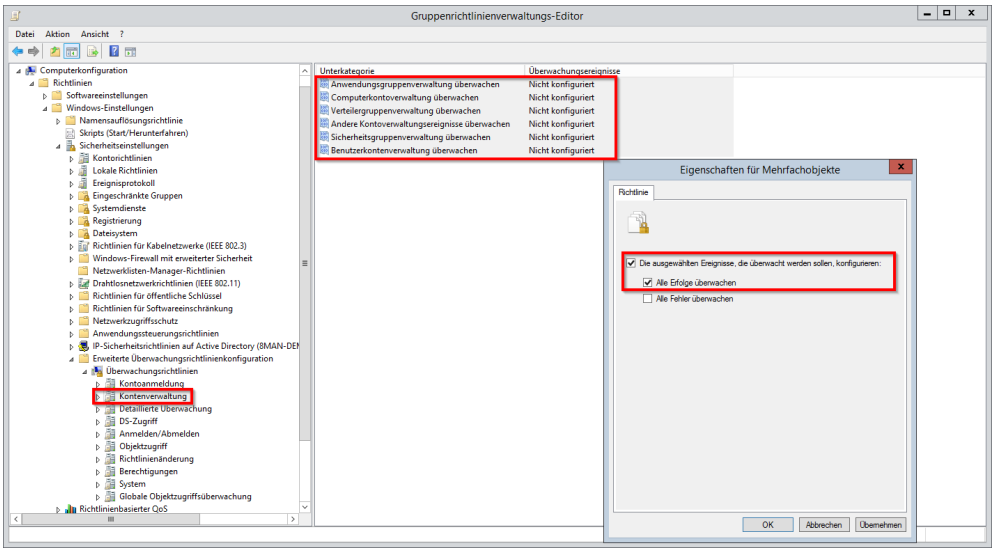


Navigieren Sie zu "Sicherheitsoptionen".

Wählen Sie die Richtlinie "Überwachung: Unterkategorie...".

Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Sicherheitsrichtlinie wie gezeigt.

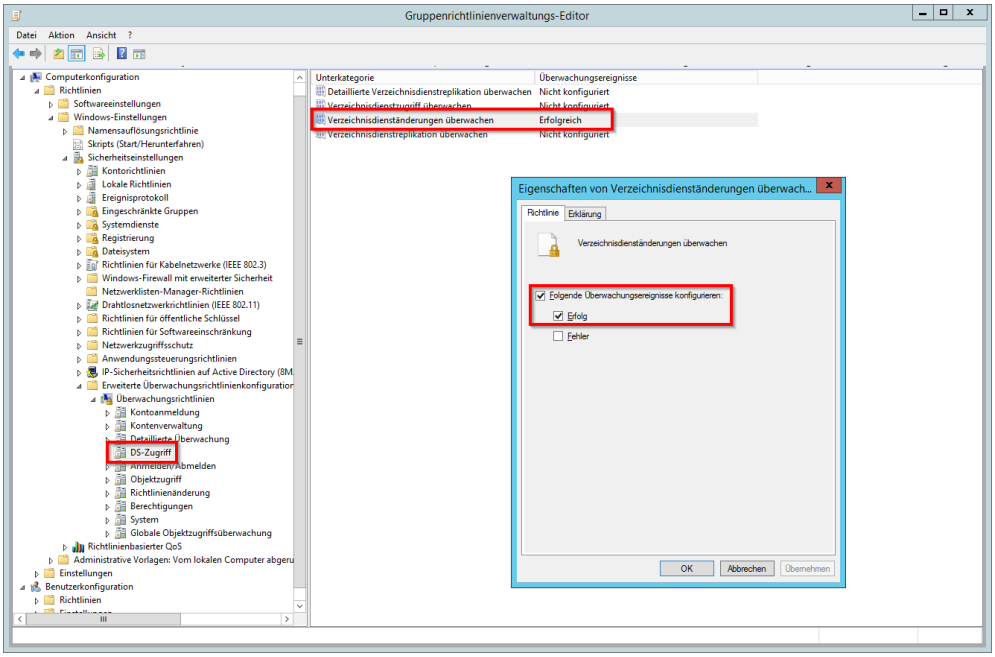
Die Reihenfolge, in der Sie die Optionen setzen, beeinflusst die Wirksamkeit der Richtlinie. Halten Sie die hier vorgegebene Reihenfolge ein!



Navigieren Sie zu Kontenverwaltung.

Nutzen Sie die Mehrfachauswahl und markieren alle Unterkategorien.

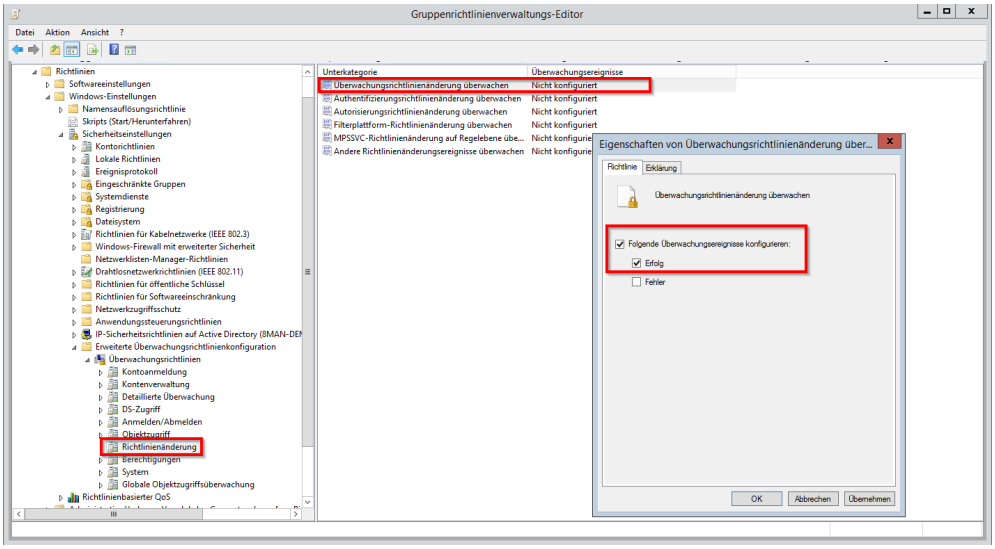
Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Überwachung bei Erfolg wie gezeigt.



Navigieren Sie zu "DS-Zugriff".

Wählen Sie die Unterkategorie "Verzeichnisdienständerungen überwachen".

Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Überwachung bei Erfolg wie gezeigt.



Navigieren Sie zu "Richtlinienänderung".

Wählen Sie die Unterkategorie "Überwachungsrichtlinienänderung überwachen".

Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Überwachung bei Erfolg wie gezeigt.

Nachdem Sie die Einstellungen vorgenommen haben:

- führen Sie ein manuelles Richtlinienupdate mit dem Kommando
  gpupdate /force
  aus,
- prüfen Sie die Ausführung der Überwachungsrichtlinien.

3.1.1.1.3 Den AD Logga Speicherplatzbedarf konfigurieren

Für 1.000 Ereignisse werden ca. 0,57 MB Speicherplatz in der Datenbank benötigt.

Die Vorhaltedauer für AD Logga Einträge beträgt standardmäßig 30 Tage und kann unter Server -> Datenstandspeicherung geändert werden.

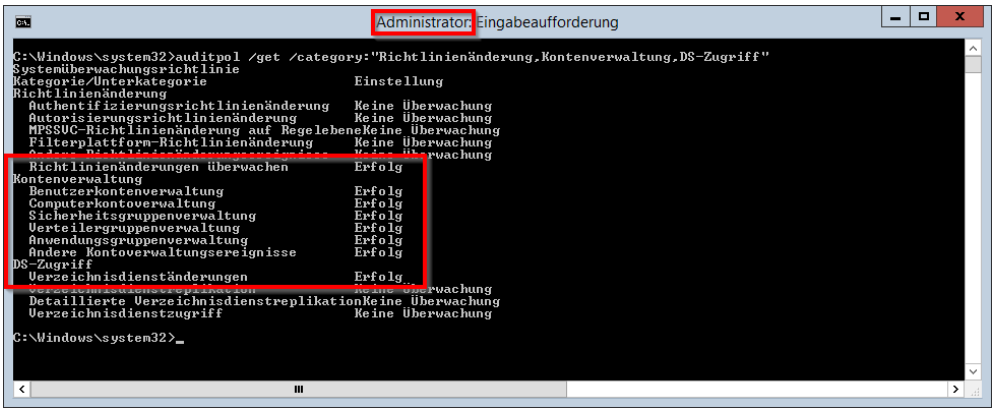
3.1.1.1.4 Die Ausführung der Überwachungsrichtlinien überprüfen

Um die Ausführung der Überwachungsrichtlinie zu überprüfen, starten Sie eine Eingabeaufforderung mit Administratorrechten und führen folgendes Kommando aus:

```
auditpol /get /category:"Richtlinienänderung,Kontenverwaltung,DS-Zugriff"
```

alternativ für alle Kategorien oder andere Sprachen:

```
auditpol /get /category:*
```



Die markierten Unterkategorien müssen auf "Erfolg" eingestellt sein.

3.1.1.2 Größe des Windows Security Logs festlegen

Um keine Ereignisse zu "verlieren", muss je nach Ereignisaufkommen die maximale Größe für das Security Event Log eingestellt werden. Für die betreffenden Überwachungseinstellungen belegt ein Ereignis im Durchschnitt etwa 1 KB.

Beispiel:
Für eine Serverausfall- bzw. Wartungszeit (des als AD Logga Kollektor gewählten Servers) von z.B. einer Stunde bei 1.000 Ereignissen pro Stunde läge das absolute Minimum der Security Event Log Größe also bei 1 MB. In Anbetracht dieser geringen Speicheranforderung für 1.000 Ereignisse, der Unbestimmtheit von Ausfallzeiten, sowie der Relevanz von Security Ereignissen, empfehlen wir, hier reichlich zu dimensionieren.

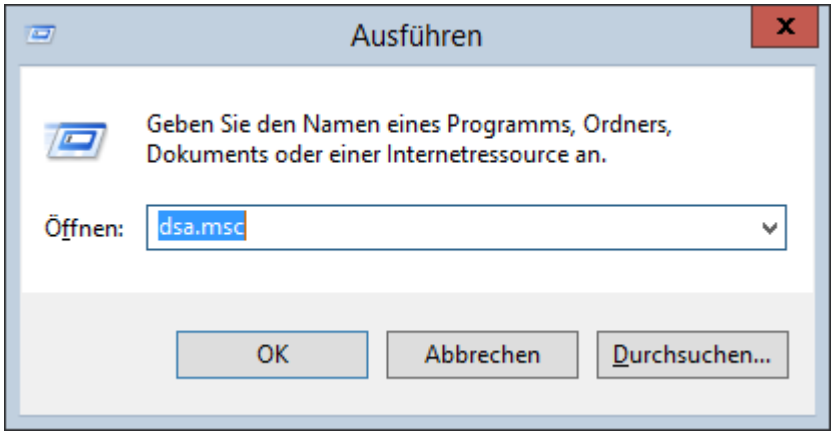
Wie Sie die Größe einstellen, finden Sie bei Microsoft.

3.1.1.3 Die Überwachungsrechte in den AD-Objekt-SACLs einrichten

Nachdem Sie die Überwachungsrichtlinien aktiviert haben, müssen Sie die Überwachungsrechte für die AD-Objekte (SACL) entsprechend konfigurieren.

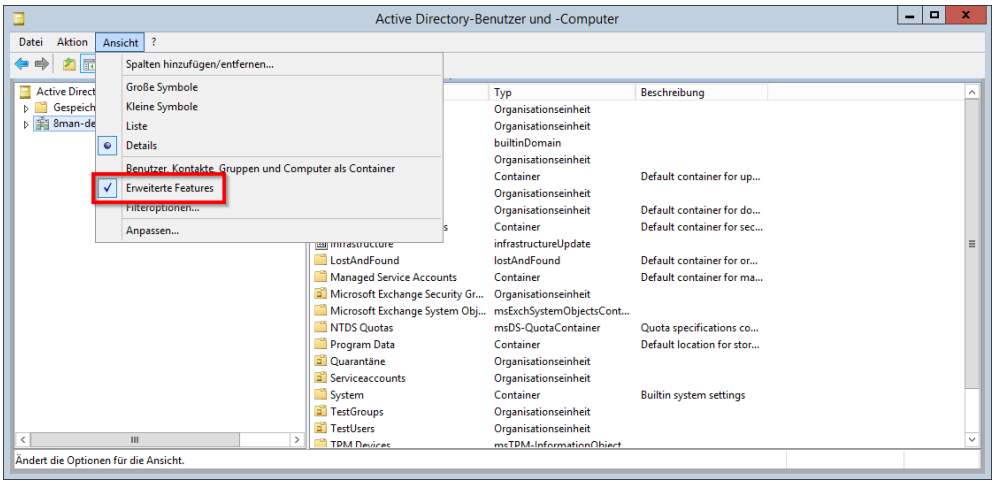
Für die Konfiguration der SACL ist das User Recht "Manage Auditing and Security Log" notwendig (was dem Privileg "SeSecurityPrivilege" entspricht). Dazu müssen Sie Mitglied der Gruppe "Ereignisprotokollleser" oder "Domänen-Admins" sein.

Die Einrichtung der SACL ist nur auf einem der zur überwachenden Domäne gehörenden DC notwendig. Die anderen DCs erhalten diese dann über die Replikation.

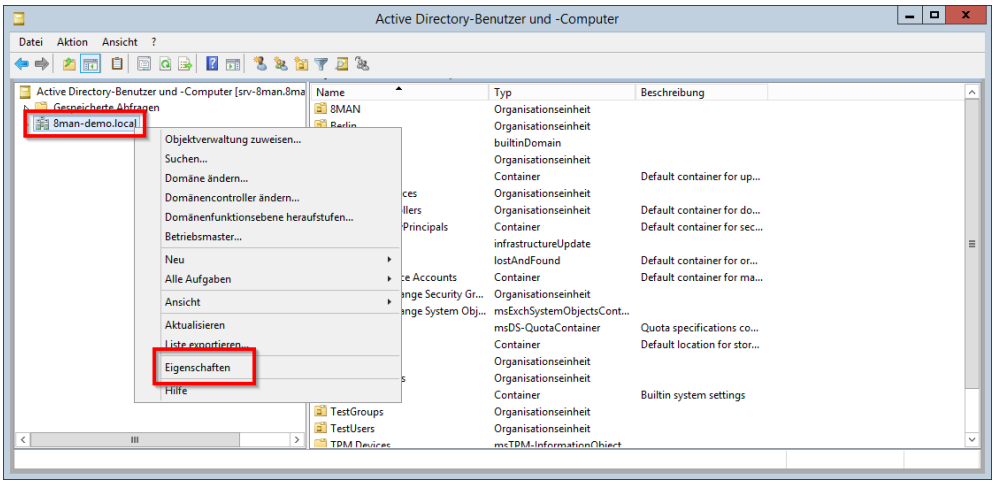


Starten Sie die Verwaltung der Active Directory-Benutzer und -Computer auf einem DC, z.B. mit dem Kommando

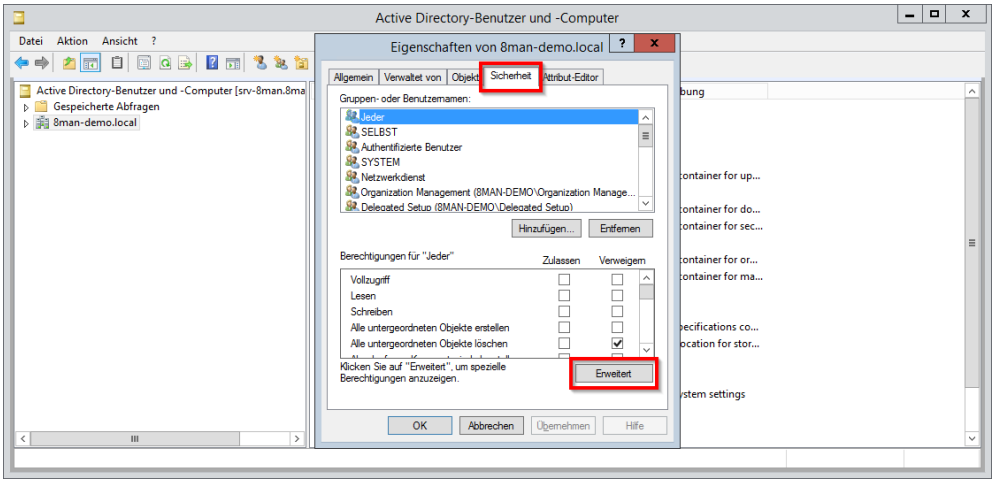
dsa.msc



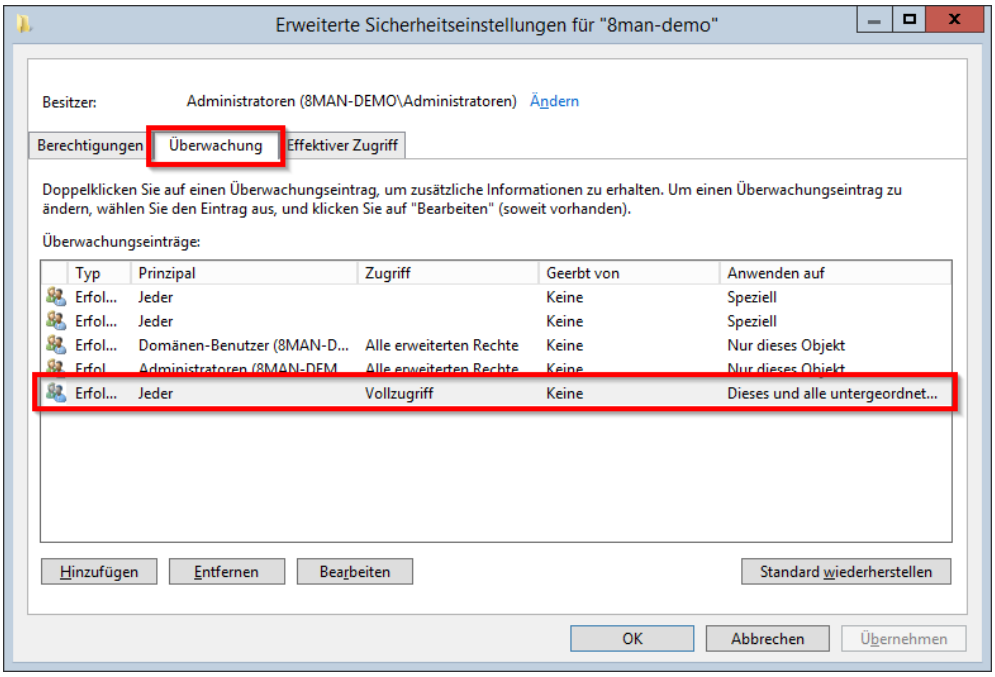
*Aktivieren Sie die Option "**Ansicht > Erweiterte Features**".*



*Wählen Sie die zu überwachende Domäne mit Rechtsklick und dann "**Eigenschaften**".*



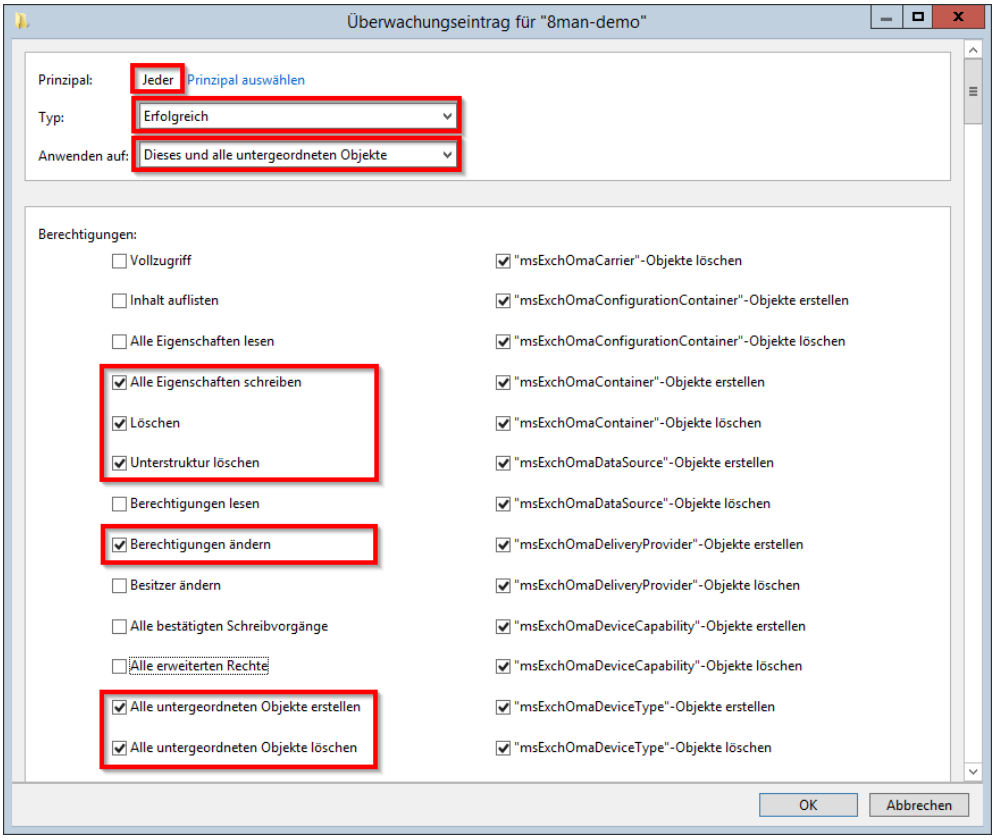
*Wählen Sie im Eigenschaftenfenster den Reiter "**Sicherheit**" und dann die Schaltfläche "**Erweitert**".*



Wählen Sie den Reiter "Überwachung".

Analysieren Sie die bereits vergebenen Überwachungsrechte. Vielleicht sind ja schon ausreichende Rechte vergeben?

Erweitern Sie ggf. die Berechtigungen eines vorhandenen "Jeder"- Prinzipals oder fügen Sie einen Eintrag hinzu.



Benötigt wird mindestens:

Prinzipal: "Jeder"

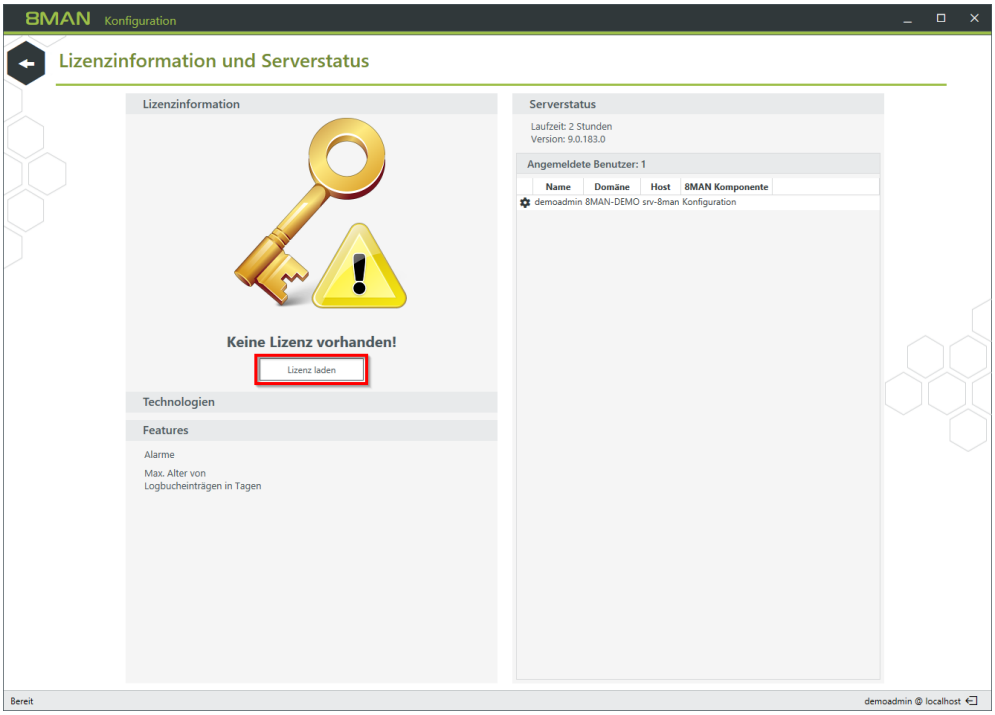
Typ: "Erfolgreich"

Anwenden auf: "Dieses und alle untergeordneten Objekte"

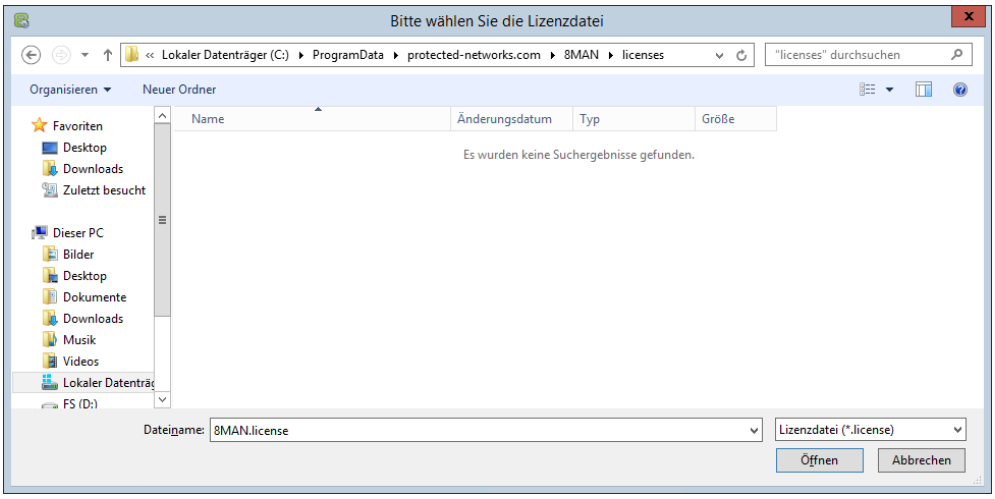
Berechtigungen:

- *Alle Eigenschaften schreiben*
- *Löschen*
- *Unterstruktur löschen*
- *Berechtigungen ändern*
- *Alle untergeordneten Objekte erstellen*
- *Alle untergeordneten Objekte löschen*

3.1.2 Die Produktlizenz laden



Klicken Sie in der 8MAN Konfiguration im Menü Serverstatus auf Lizenz laden.

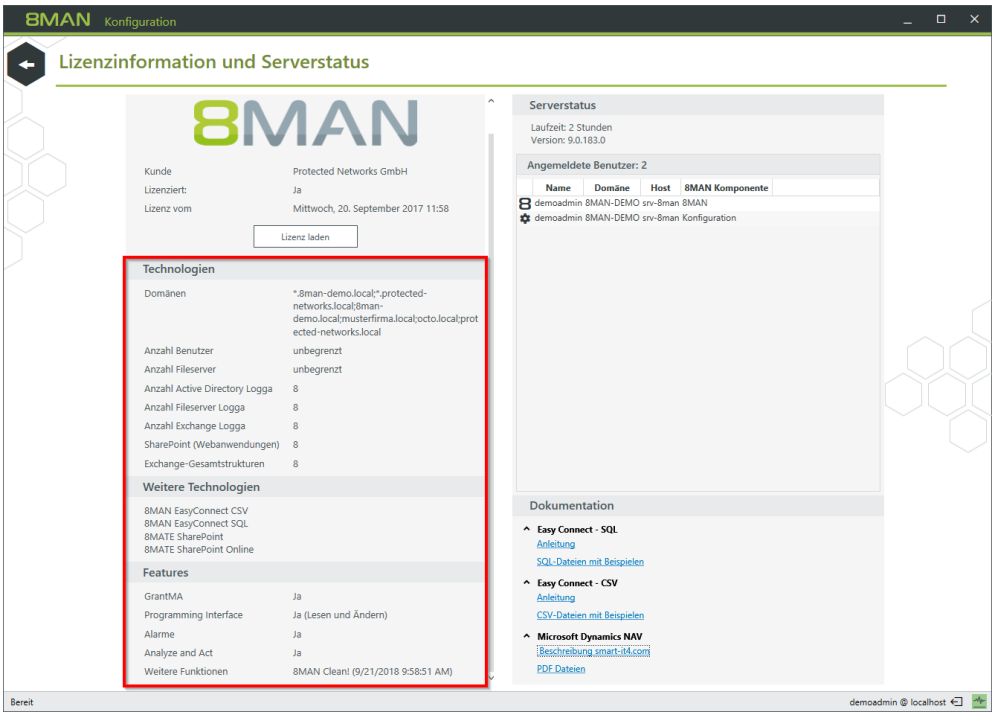


Wählen Sie den Pfad zu Ihrer Lizenzdatei.

8MAN Lizenzdateien haben die Endung ".license".

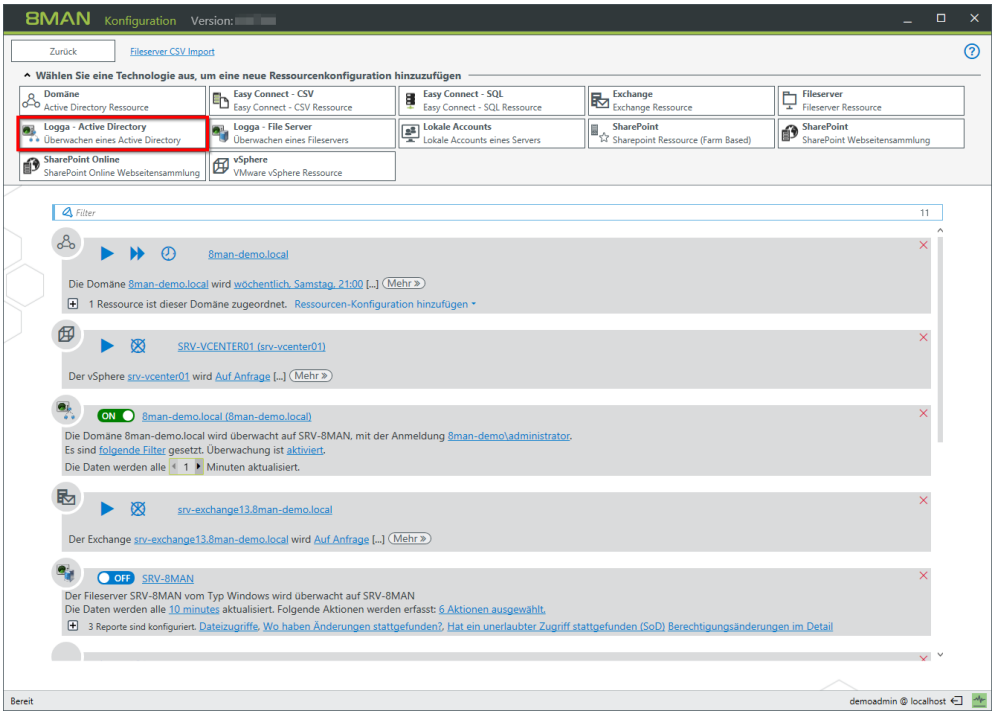
Nach dem Klick auf Öffnen wird die Lizenzdatei nach **`%ProgramData%protected-networks.com\8MAN\licenses`** *kopiert.*

Alle lizenzierten Features werden sofort aktiviert.



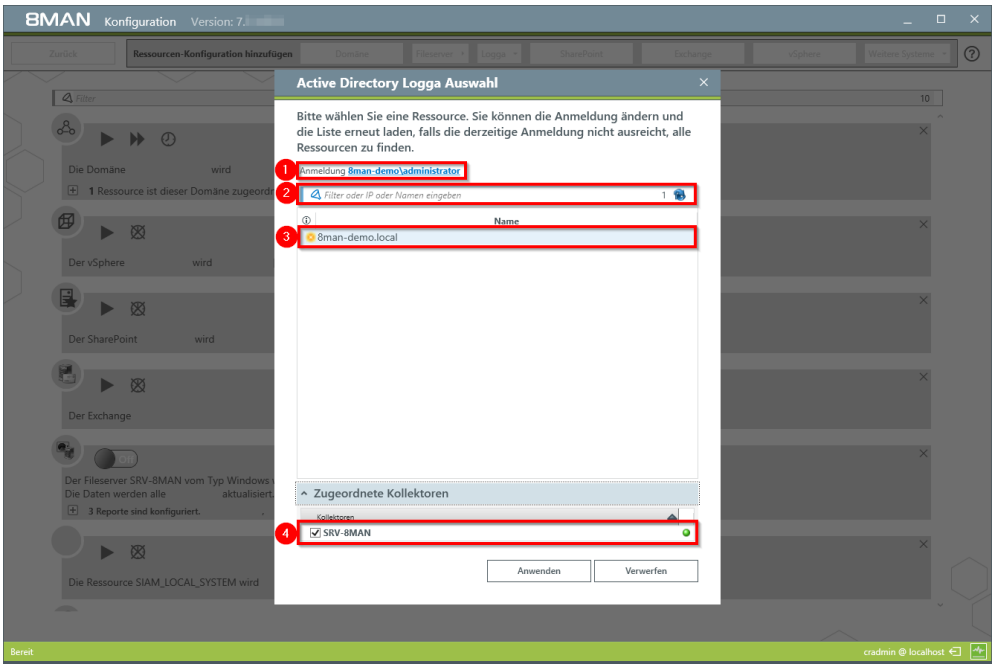
Haben Sie die Lizenz erfolgreich geladen, sehen Sie detaillierte Informationen zum Lizenzumfang.

3.1.3 Eine AD Logga Konfiguration hinzufügen



Wählen Sie auf der Startseite der Konfiguration "Scans".

Wählen Sie "Logga - Active Directory".

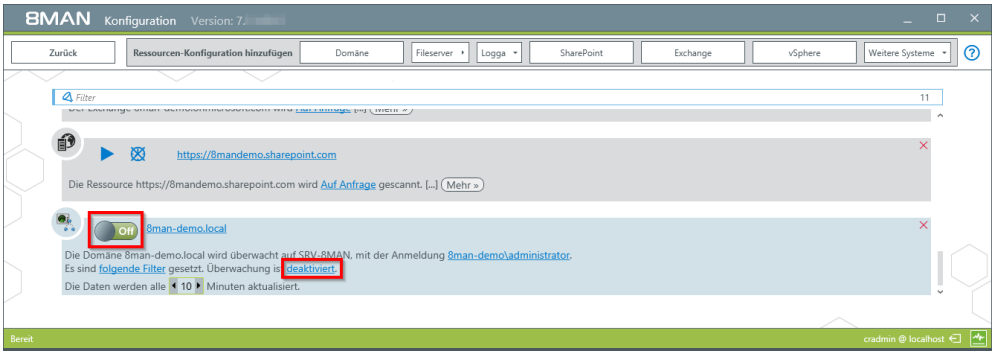


1. *Geben Sie gültige Anmeldeinformationen für die Domäne an, die überwacht werden soll.*
2. *Nutzen Sie den Filter, um die gewünschte Domäne zu finden.*
3. *Selektieren Sie eine Domäne. Child-Domänen werden nicht mit überwacht. Jede Domäne muss separat konfiguriert werden.*
4. *Wählen Sie einen Kollektor-Server. Sie können nur einen Kollektor pro Domäne wählen.*

Wenn Sie eine AD Logga Konfiguration hinzugefügt haben, ist der Logga zunächst deaktiviert.

Sie müssen den AD Logga aktivieren, um Ereignisse aufzuzeichnen.

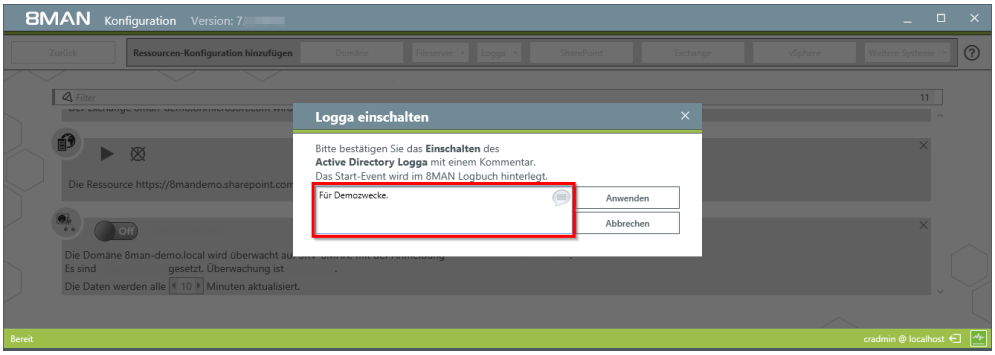
3.1.4 Den AD Logga aktivieren/deaktivieren



Wählen Sie auf der Startseite der Konfiguration "Scans".

Klicken Sie in der gewünschten AD Logga Konfiguration auf den Schalter oder den Link, um den AD Logga zu aktivieren.

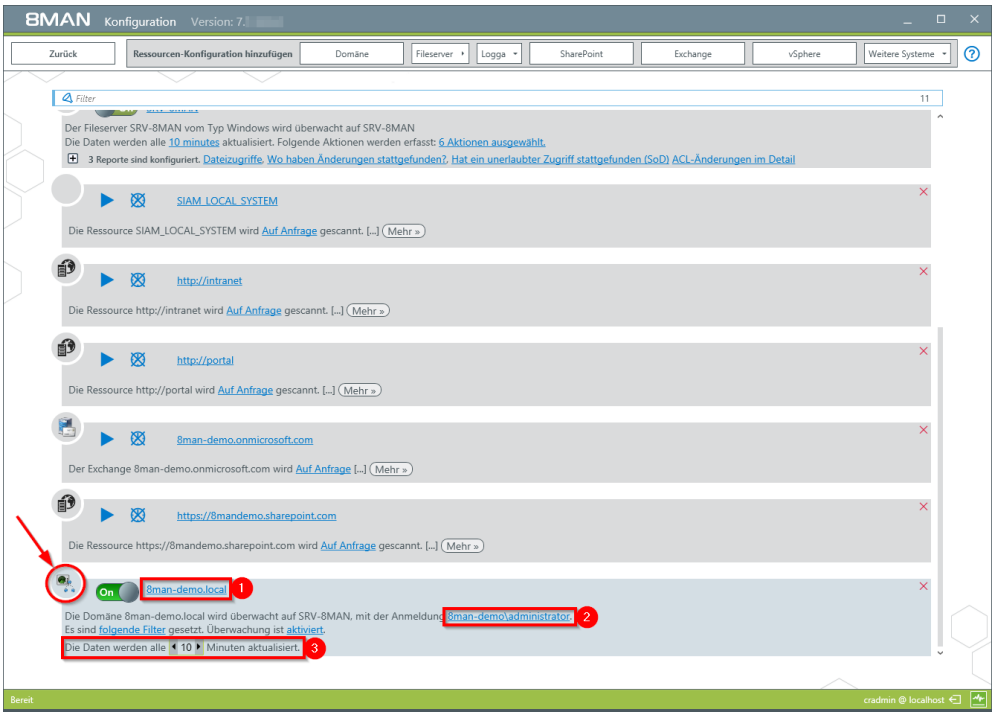
AD Logga Ereignisse werden standardmäßig 30 Tage gespeichert. Siehe Vorhaltedauer für Datenstände konfigurieren



Sie müssen einen Kommentar eingeben.

Gehen Sie für das Deaktivieren analog vor.

3.1.5 Eine AD Logga Konfiguration anpassen



Wählen Sie auf der Startseite der Konfiguration "Scans".

1. *Geben Sie der Konfiguration einen anderen Namen.*
2. *Hinterlegen Sie die Anmeldung, mit welcher der AD Logga die Ereignisse von den DCs liest. Das Konto muss Mitglied in der Gruppe "Ereignisprotokollleser" oder "Domänen-Admins" sein. Sie können die Anmeldung nur ändern, wenn der Logga ausgeschaltet ist.*
3. *Legen Sie fest, in welchem Intervall die Logga Daten aktualisiert werden. Ereignisse werden vom Kollektor zwischengespeichert und in dem eingestellten Intervall über den 8MAN Server in die Datenbank geschrieben. Standardeinstellung: 10 min,*

Mögliche Werte 1 bis 60 Minuten.

3.1.5.1 AD Logga Ereignisse filtern

Filtern Sie uninteressante Ereignisse heraus, um nur relevante Einträge aufzuzeichnen. Filtern bedeutet hier, dass herausgefilterte Ereignisse nicht aufgezeichnet werden.
Sie erhöhen damit deutlich den Überblick und reduzieren Datenvolumen. Ein typisches Beispiel sind die häufigen Attributänderungen des Exchange-Servers.

Sie können einen Filter nur konfigurieren, wenn ein AD-Scan vorhanden ist.

3.1.5.1.1 Die Filterprinzipien verstehen

Der AD Logga Filter ist als Blacklist-Filter konzipiert. Blacklist bedeutet hier: Der AD Logga zeichnet mit maximalem Umfang auf. Sie legen fest, welche Ereignisse nicht aufgezeichnet - also verworfen - werden.
Standardmäßig ist ein Filter auf die zwei Objektklassen "Service-Connection-Point" und "Print-Queue" gesetzt.

Die Filter-Kriterien arbeiten additiv. Ein Ereignis wird verworfen, wenn Kriterium 1 oder Kriterium 2 oder Kriterium 3 zutrifft, oder auch mehrere Kriterien gleichzeitig.

Die Filter-Kriterien stehen in keiner Korrelation zueinander. Die Ereignisse werden vom AD Logga nacheinander bezüglich der Kriterien bewertet. Bei einem Treffer wird das Ereignis sofort verworfen und nicht weiter überprüft, unabhängig davon, ob ein anderes Kriterium schon bewertet wurde oder nicht.

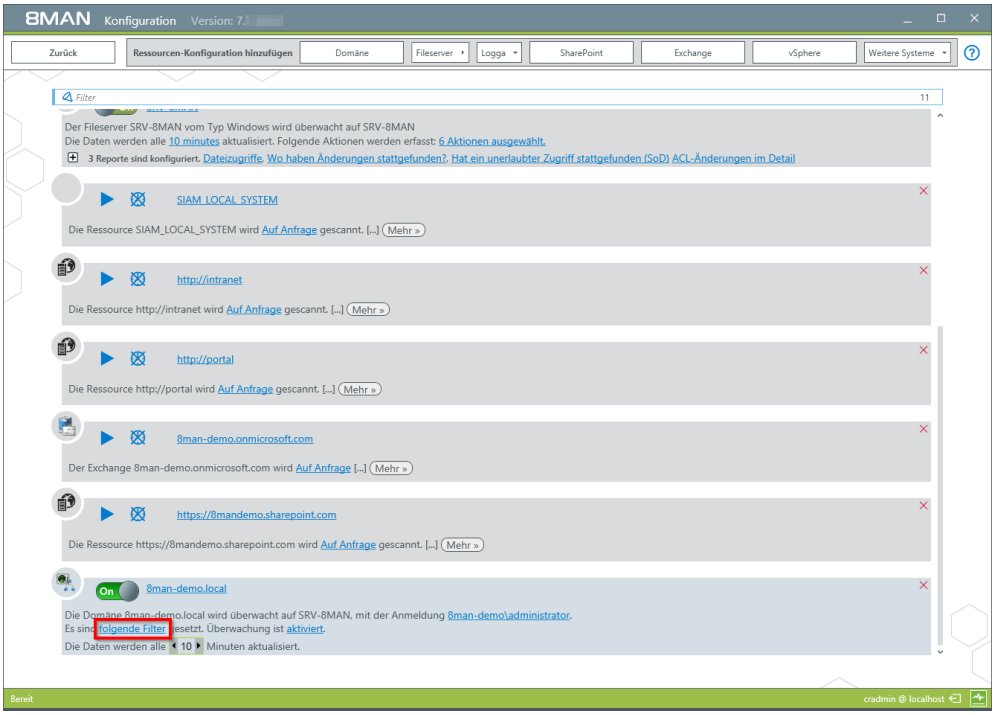
Beispiele:

- Ist Benutzer A als Filter konfiguriert, dann werden alle von ihm im AD vorgenommen Änderungen verworfen, auch wenn die von ihm geänderte Objektklasse oder das geänderte Attribut nicht als Filter konfiguriert sind. Änderungen, die Benutzer A selbst betreffen, werden weiterhin aufgezeichnet.

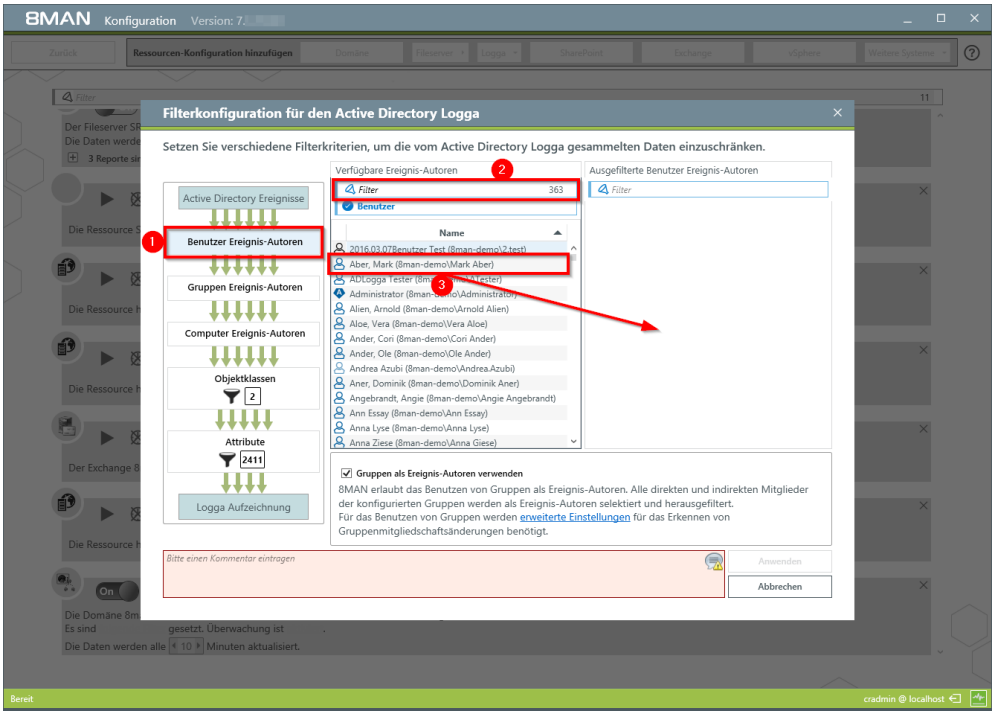
- Ist Objektklasse X als Filter konfiguriert, dann werden alle Ereignisse, die explizit diese Objektklasse enthalten, verworfen, auch wenn der Ereignis-Autor oder das geänderte Attribut nicht als Filter konfiguriert sind. Analog gilt dies auch für den Attribut-Filter.

Hinweis:
Nicht alle Security-Log Ereignisse enthalten die betroffene Objektklasse oder das betroffene Attribut. So werden z.B. Mitgliedschaftsänderungen nicht verworfen, selbst wenn die Objektklassen „User“ und „Group“ und das Attribut „Member“ als Filter konfiguriert sind.

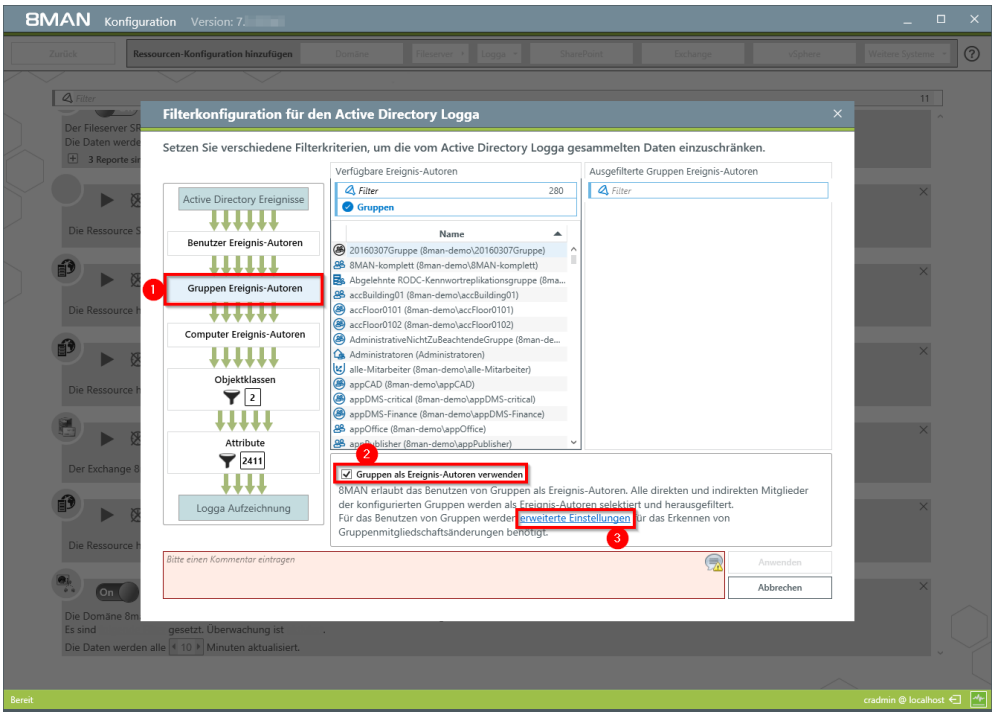
3.1.5.1.2 Die Ereignisfilter konfigurieren



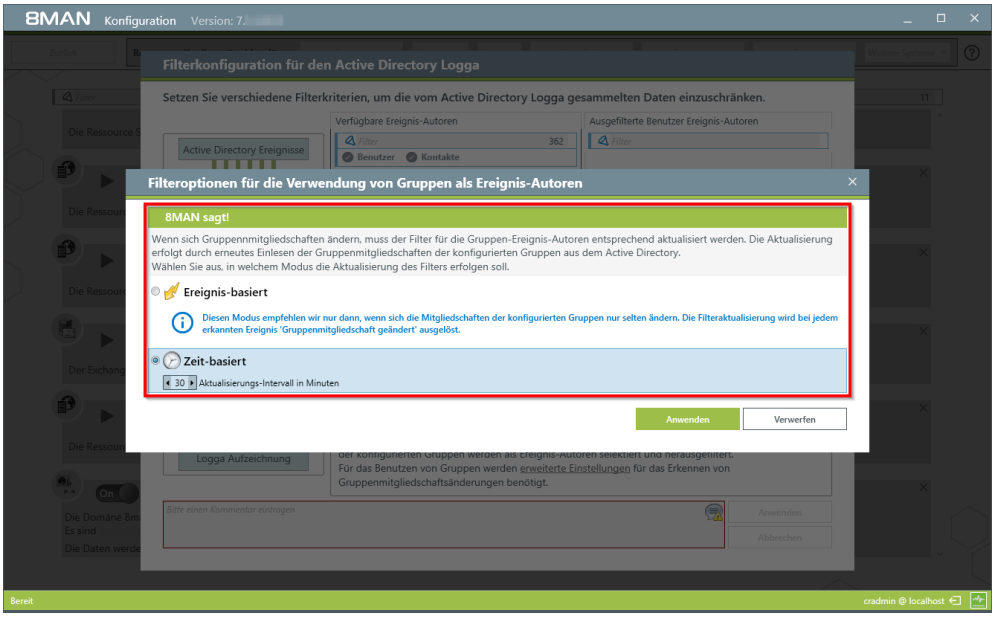
Klicken Sie auf den Link.



1. *Filtern Sie Ereignisse von Benutzern heraus.*
2. *Nutzen Sie den Filter, um die gewünschten Benutzer zu finden. Sie können nach Anzeigename (Display Name) oder CommonName suchen.*
3. *Selektieren Sie einen Benutzer und ziehen diesen per Drag&Drop in die rechte Spalte.*



1. *Sie können Gruppen als Ereignis-Autoren herausfiltern. Die Filterstufe wird angezeigt, wenn Sie*
2. *die Option aktivieren. Ziehen Sie Gruppen per Drag&Drop in die rechte Spalte, werden die Ereignisse aller Mitglieder - direkte und indirekte - herausgefiltert.*
3. *Klicken Sie auf "erweiterte Einstellungen".*

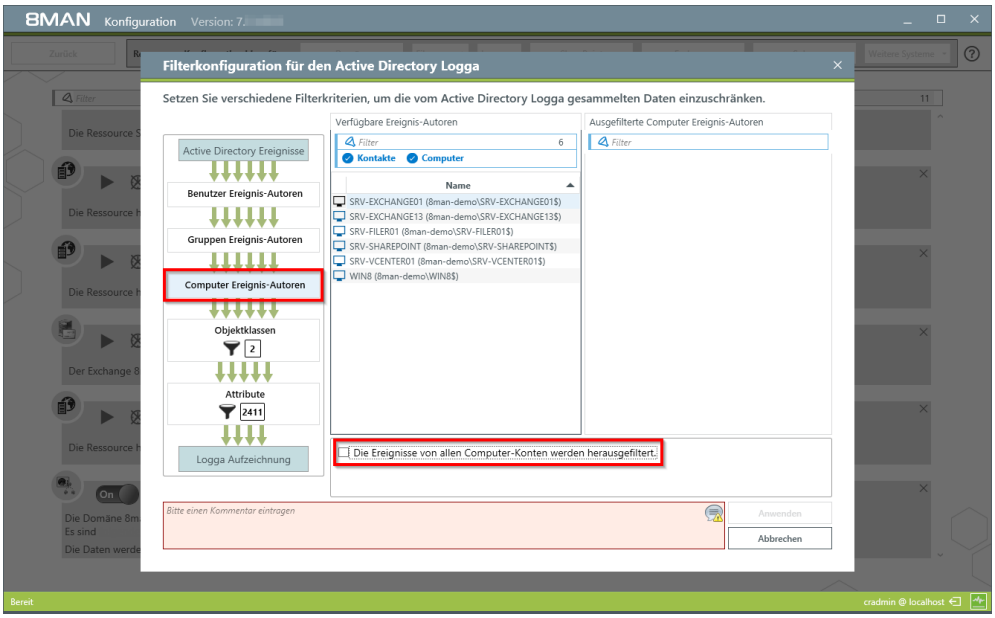


Legen Sie fest, nach welchem Modus der Filter die Gruppenmitgliedschaften aktualisiert.

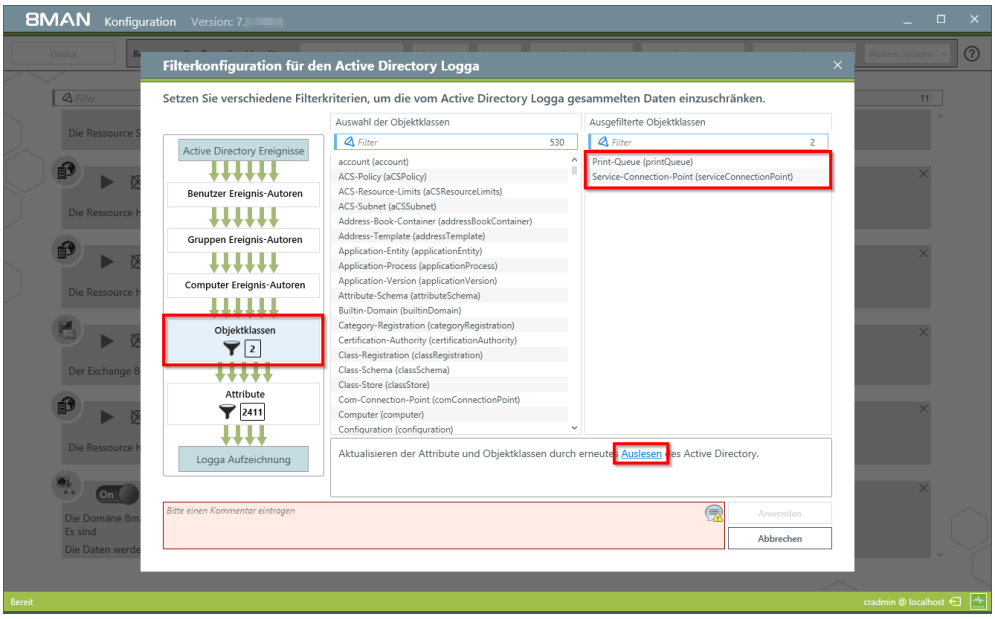
Beachten Sie die Hinweise im angezeigten Dialog.

Verwenden Sie "Ereignis-basiert" nur, wenn sich die Mitgliedschaften in den herauszufilternden Gruppen selten ändern.

Das Aktualisierungsintervall für die Option "Zeit-basiert" kann auf Werte zwischen 10 und 1440 min (24h) eingestellt werden. Je kürzer das Intervall, desto höher die Last auf dem AD.



Filtern Sie Ereignisse von einzelnen oder allen Computer-Konten heraus.

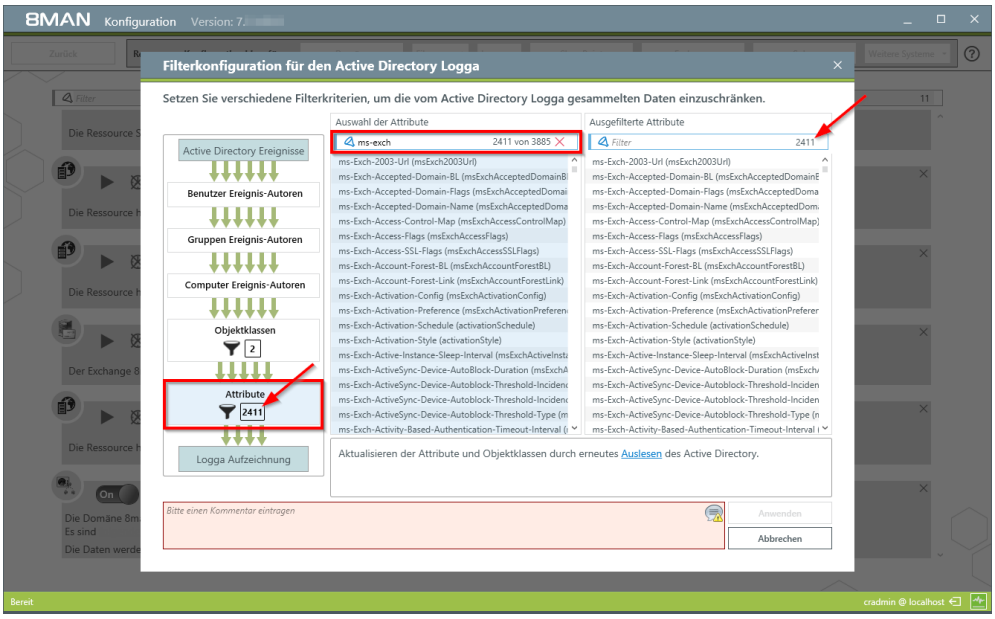


Filtern Sie Ereignisse bestimmter Objektklassen heraus.

Standardmäßig werden die Ereignisse der zwei markierten Objektklassen herausgefiltert.

Das erstmalige Laden der Objektklassen aus dem AD kann etwas Zeit in Anspruch nehmen. Danach werden die Objektklassen aus der Datenbank geladen.

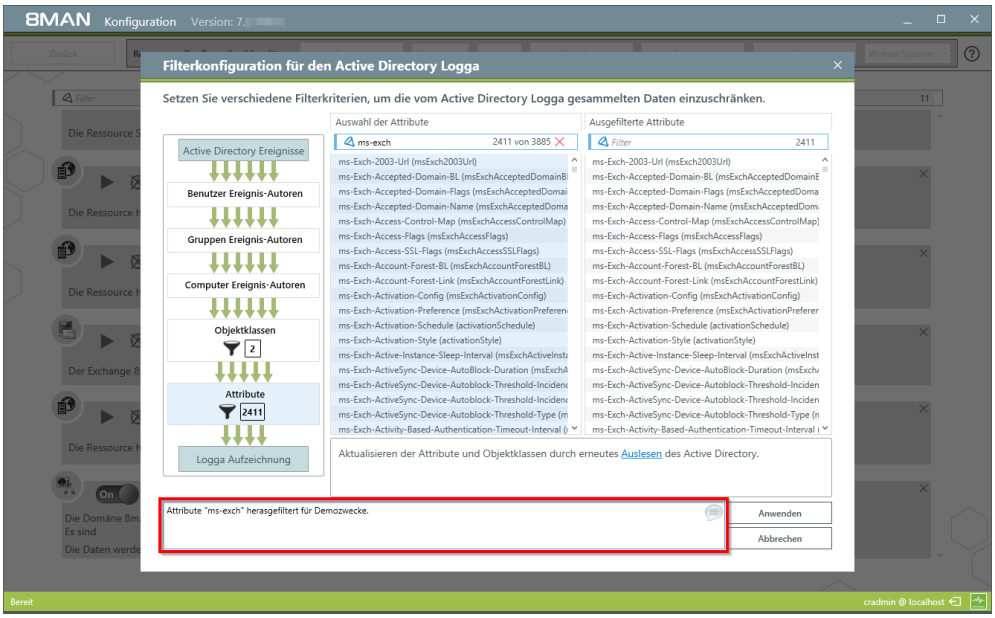
Klicken Sie auf "Auslesen", um die Objektklassen, z. B. nach einer Schema-Änderung zu aktualisieren.



Filtern Sie Ereignisse zu gewählten Attributen heraus.

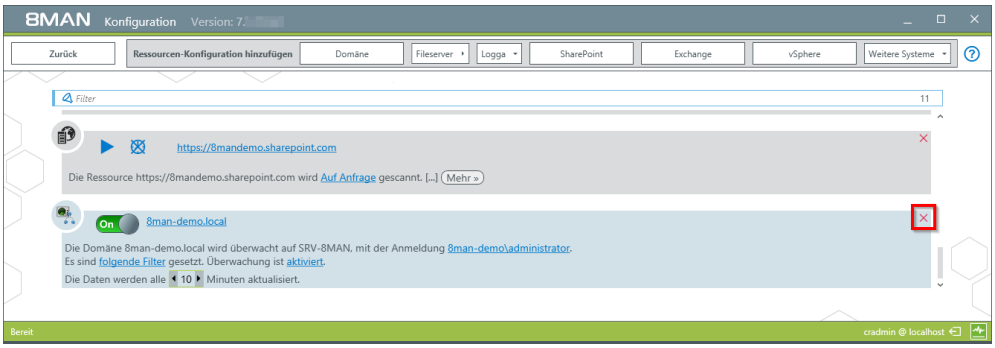
Beispiel:

Alle Ereignisse zu den Attributen, die "ms-exch" enthalten, werden herausgefiltert, also nicht aufgezeichnet.



Sie müssen einen Kommentar eingeben, um die geänderten Filtereinstellungen anzuwenden.

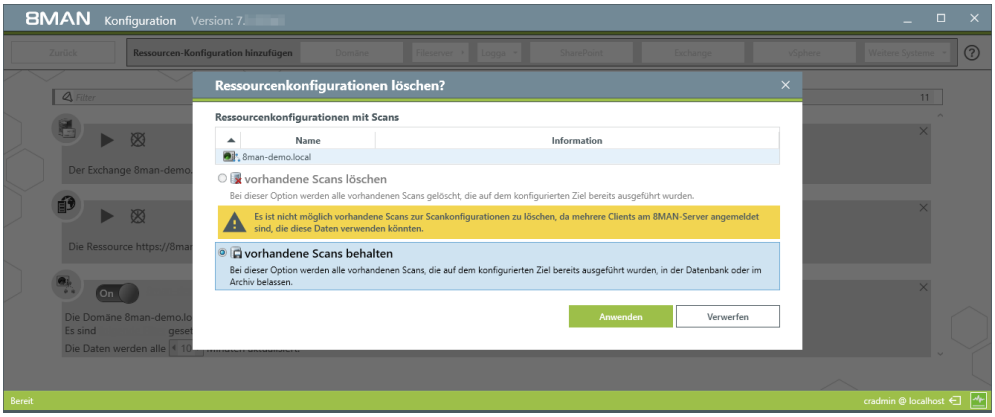
3.1.6 Eine AD Logga Konfiguration löschen



Wählen Sie auf der Startseite der Konfiguration "Scans".

Wählen Sie die gewünschte AD Logga Konfiguration.

Klicken Sie auf das rote "X".

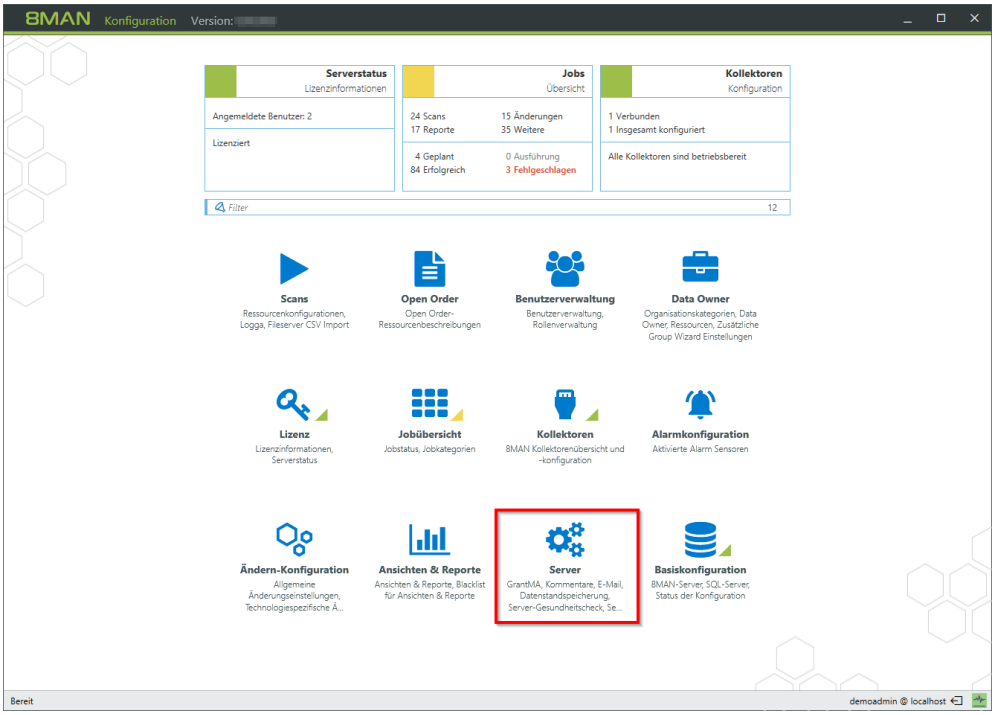


Entscheiden Sie, ob Sie vorhandene Logga-Daten behalten oder löschen wollen.

Das Löschen ist nur möglich, wenn alle weiteren Benutzeroberflächen geschlossen sind.

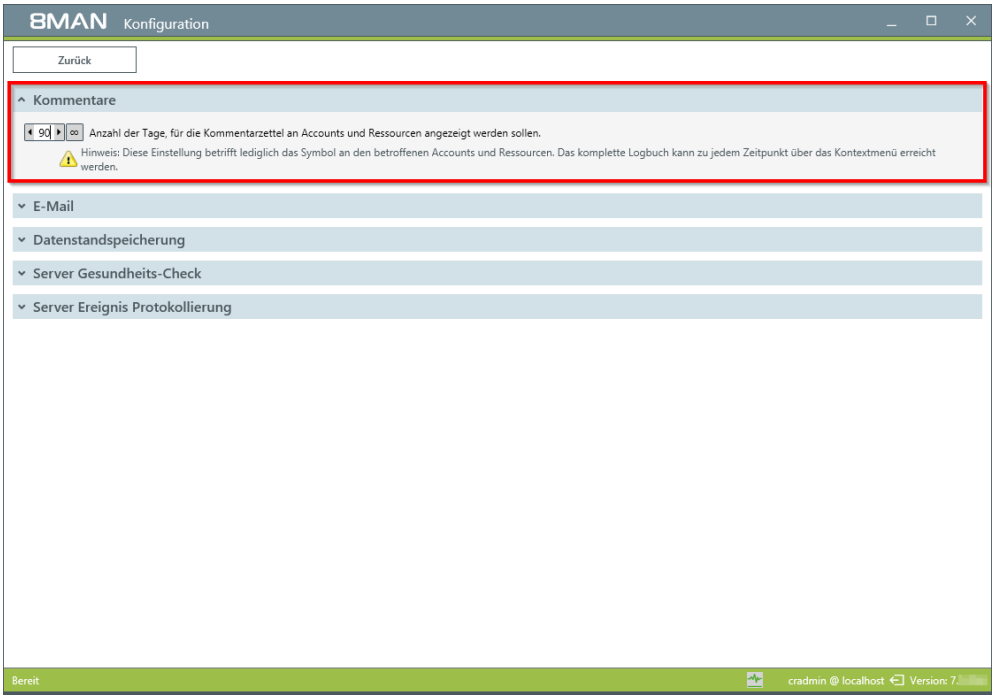
Im Menü Server-Status können Sie angemeldete Benutzer identifizieren.

4 Server



Klicken Sie auf "Server" um Einstellungen für Kommentare, E-Mail, Datenstandspeicherung, Gesundheits-Check, GrantMA und die Ereignis-Protokollierung vorzunehmen.

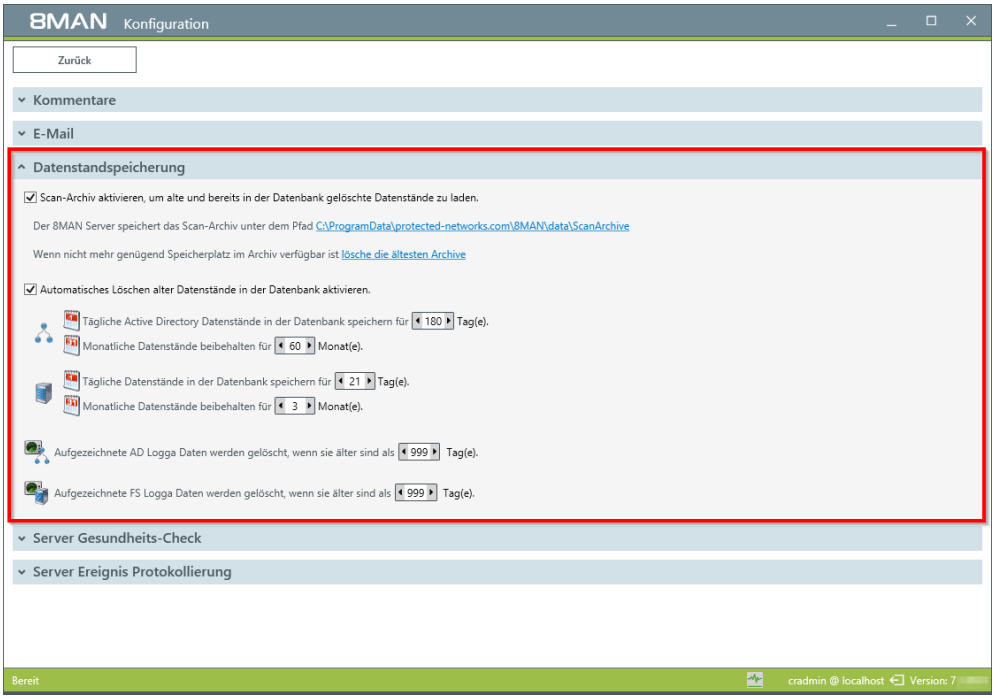
4.1 Die Anzeigedauer für Kommentarsymbole einstellen



8MAN zeigt in der Benutzeroberfläche ein Notizzettel-Symbol für hinterlegte Kommentare oder AD Logga Informationen an.

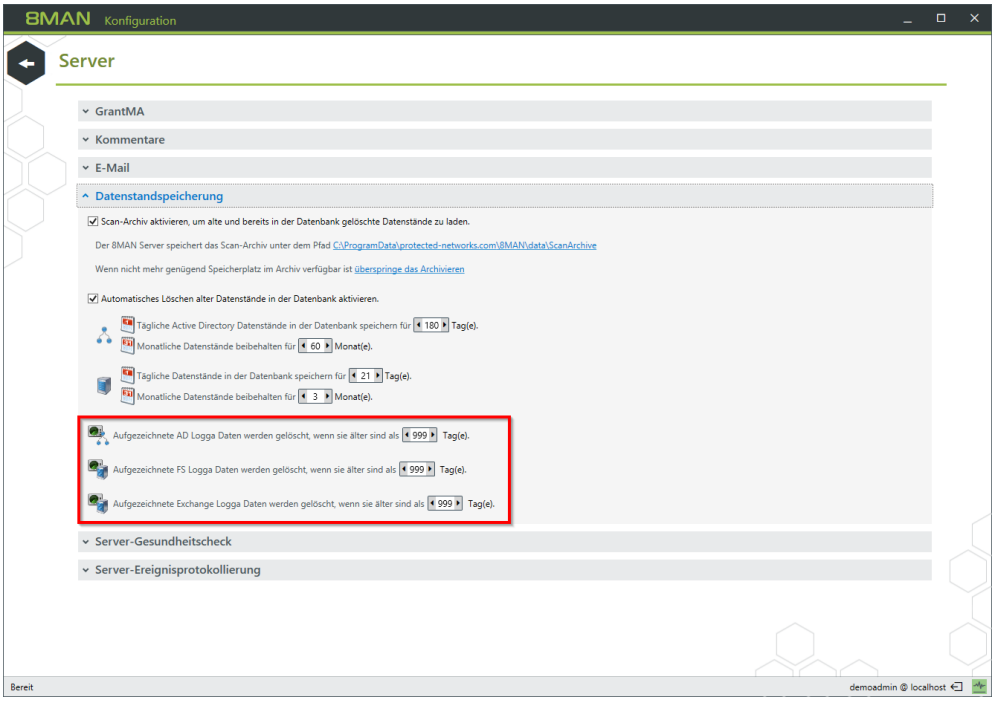
Je länger Sie 8MAN betreiben, desto mehr Notizzettel sehen Sie. Reduzieren Sie die Anzeigedauer, wenn Sie in der Benutzeroberfläche zu viele Notizzettel-Symbole sehen.

4.2 Vorhaltedauer für AD Logga Daten konfigurieren



In der Datenstandspeicherung legen Sie fest, wie lange Scan- und Logga-Daten vorgehalten werden. Sie beeinflussen damit die Größe der Datenbank und den verwendeten Speicherplatz.

Beachten Sie die Hinweise zur Verwendung von SQL Express.



Legen Sie fest, wie lange 8MAN Logga Daten vorhält.

Die Ereignisse verbrauchen folgenden Speicherplatz:
FS Logga: ca. 50 Byte
AD Logga: ca. 600 Byte

5 AD Logga Daten auswerten

5.1 Änderungen im Active Directory überwachen

Hintergrund / Mehrwert

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

Überwachung von Ereignistypen

Änderungen an:

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

Überwachung von Ereignisautoren

- Benutzer
- Gruppen
- Computer

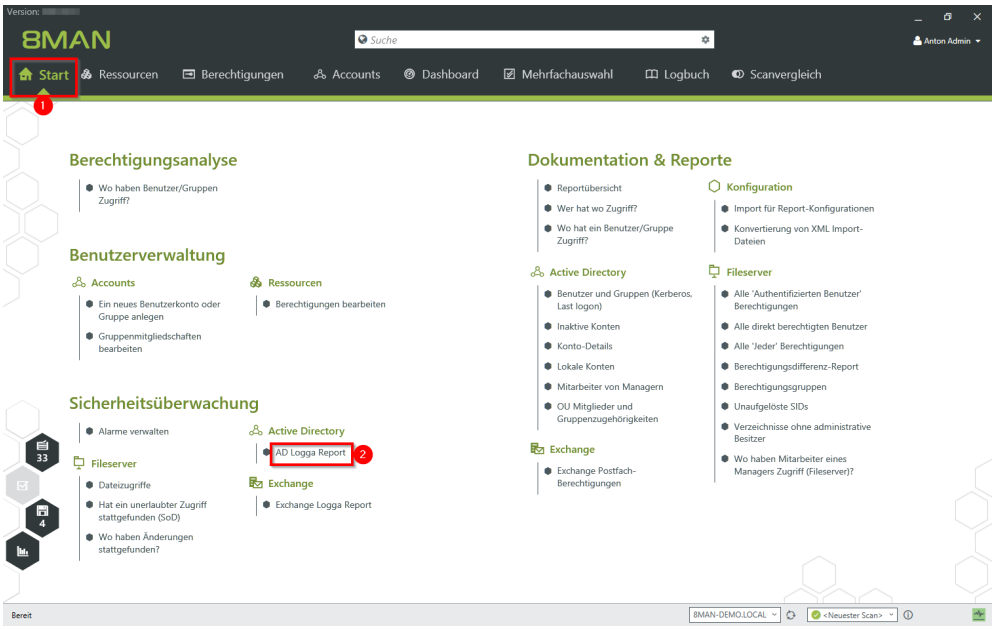
Zusätzlich können Sie noch nach Objekt Klassen und Attributen filtern. Dabei handelt es sich jedoch um Experteneinstellungen. Filtern Sie nach einem seltenen Attribut, kann dies die gesamte Suche verfremden.

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

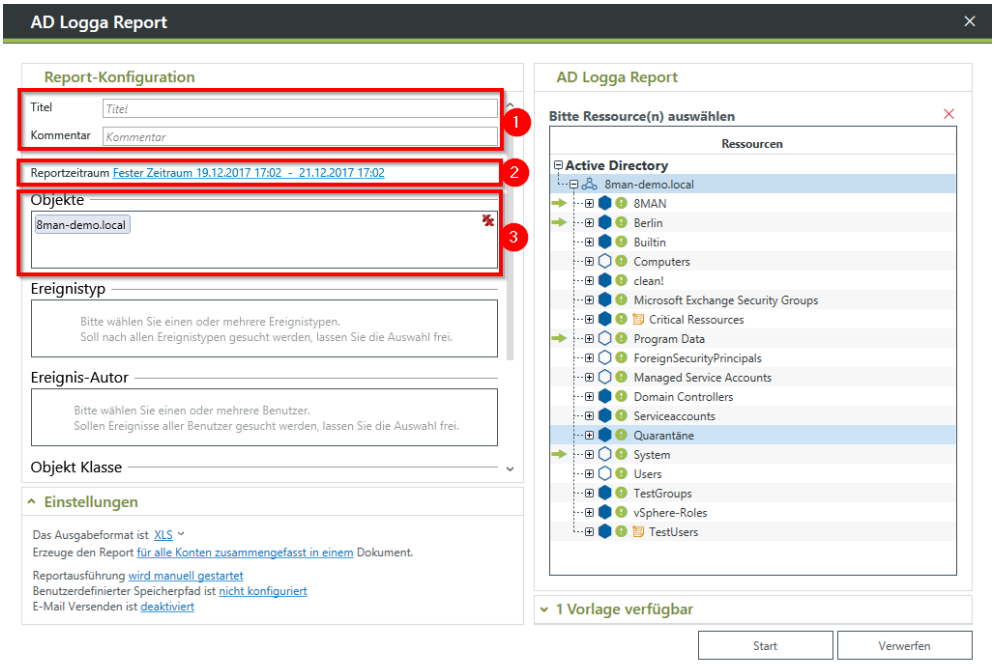
Weiterführende Services

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

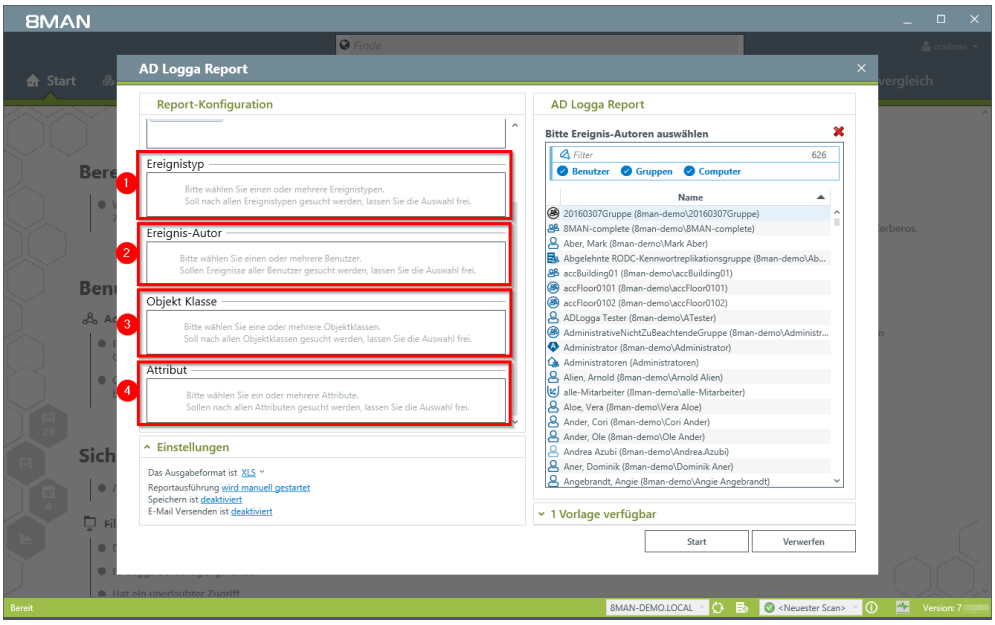
Der Prozess in einzelnen Schritten



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

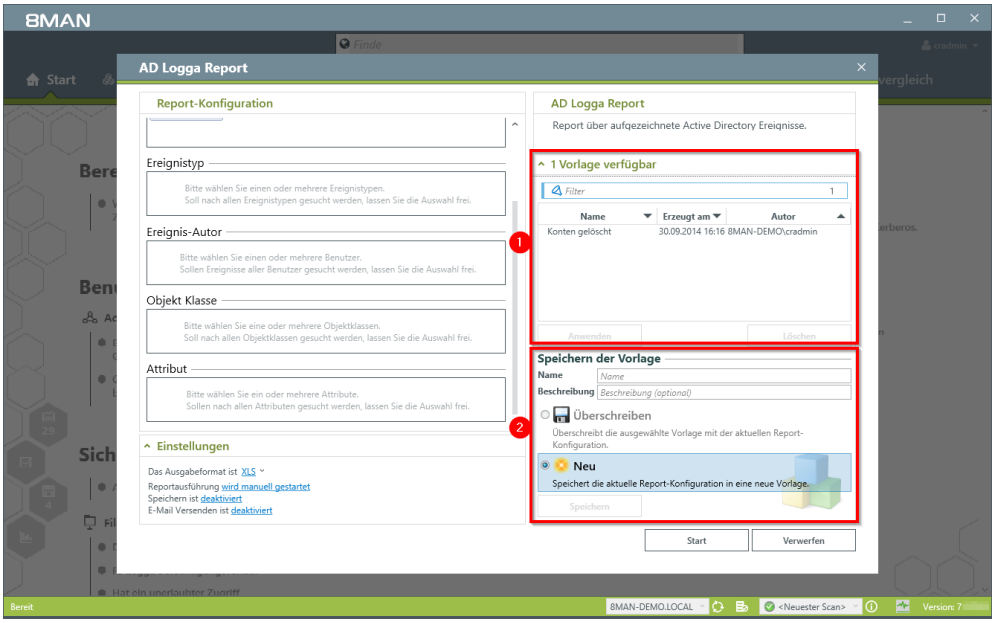


1. *Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.*
2. *Legen Sie den Zeitraum für den Report fest.*
3. *Wählen Sie die Domänenobjekte, deren Ereignisse im Report enthalten sein sollen.*



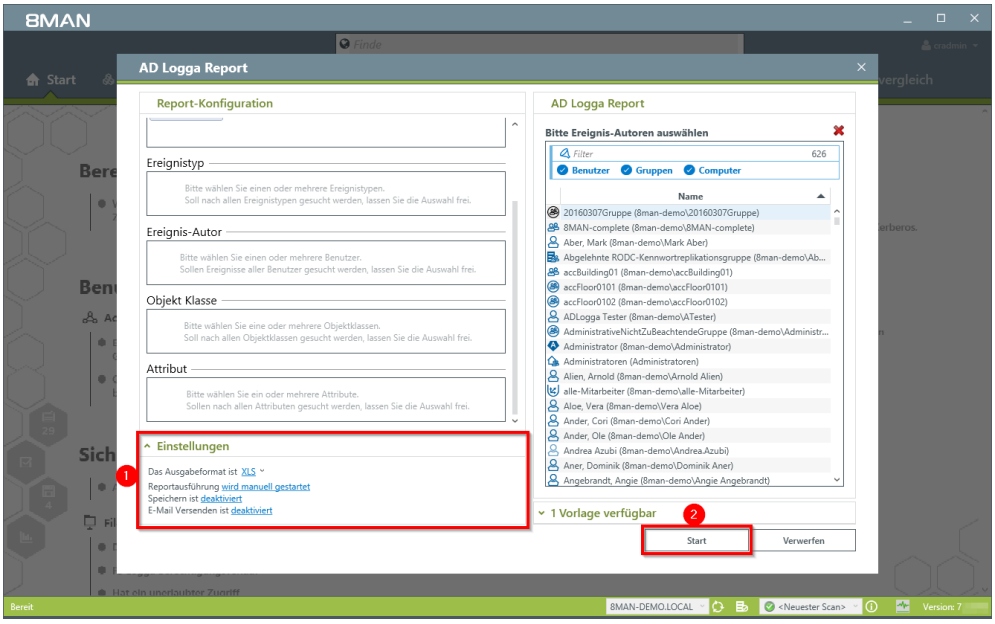
Definieren Sie den Umfang des Reports, in dem Sie die folgenden Filter setzen. Für alle Filter gilt: Sollen alle aufgezeichneten Ereignisse im Report enthalten sein, lassen Sie die Auswahl frei.

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



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

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



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

5.2 Temporäre Gruppenmitgliedschaften erkennen

Hintergrund / Mehrwert

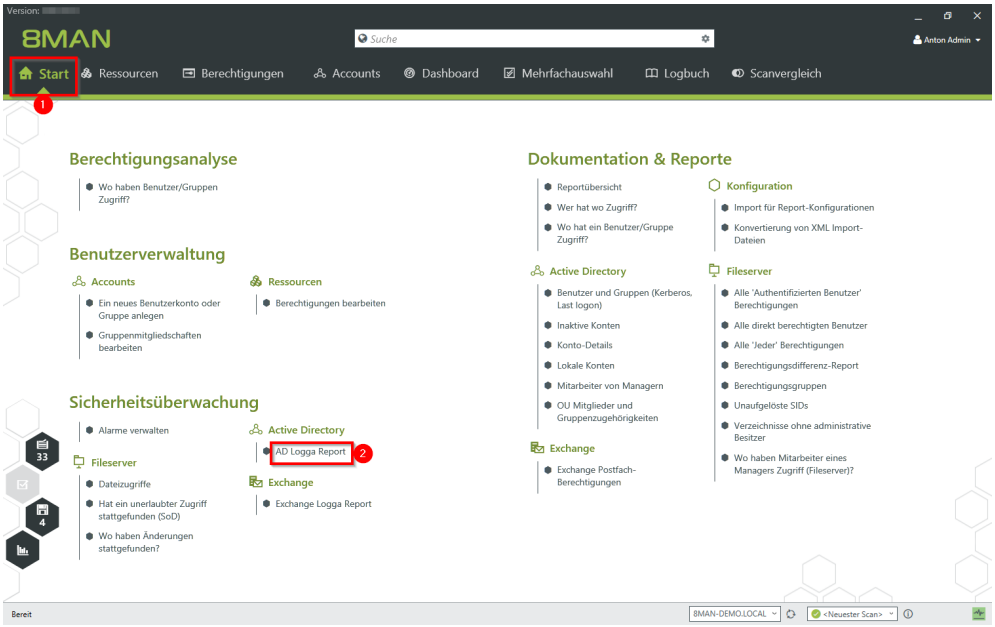
Mit dem 8MATE AD Logga schliessen Sie eine zentrale Sicherheitslücke: Temporäre Gruppenmitgliedschaften. Innentäter berechtigen sich auf geheime Verzeichnisse, kopieren Daten und stellen den Ursprungszustand der Berechtigungssituation wieder her. Ohne AD Logga bleiben Aktionen wie diese unter dem Radar.

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

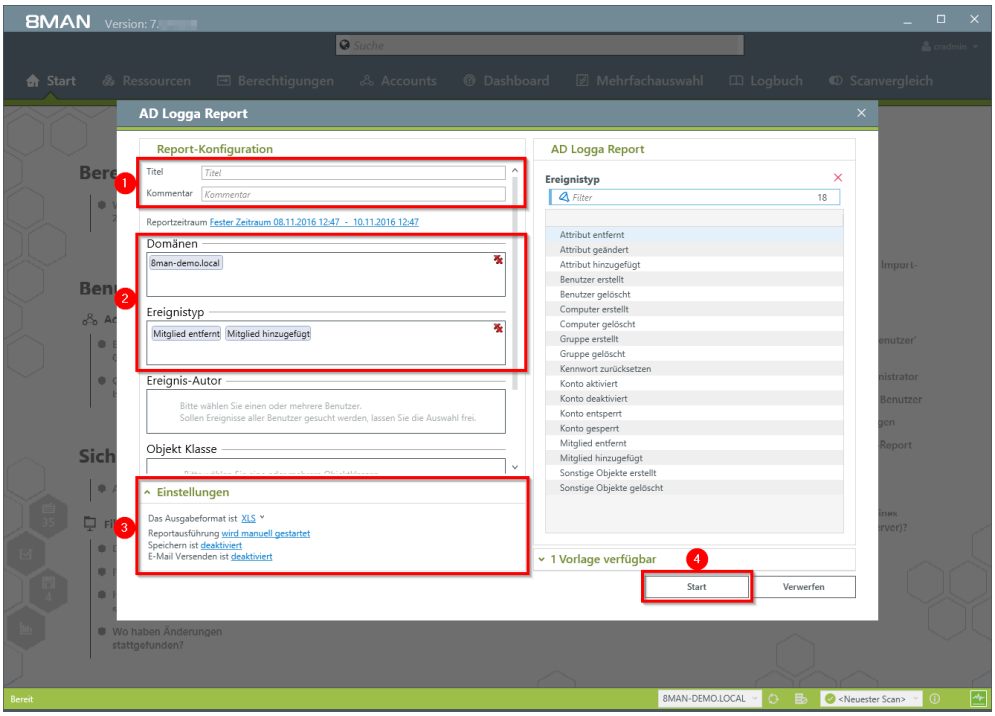
Weiterführende Services

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

Der Prozess in einzelnen Schritten



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



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

5.3 Gesperrte Benutzerkonten identifizieren

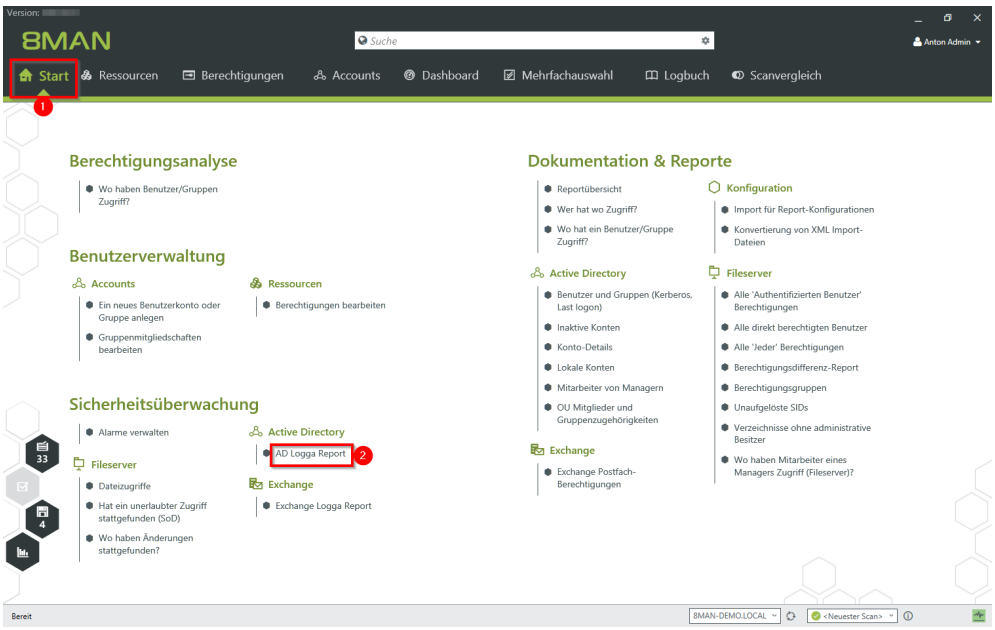
Hintergrund / Mehrwert

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

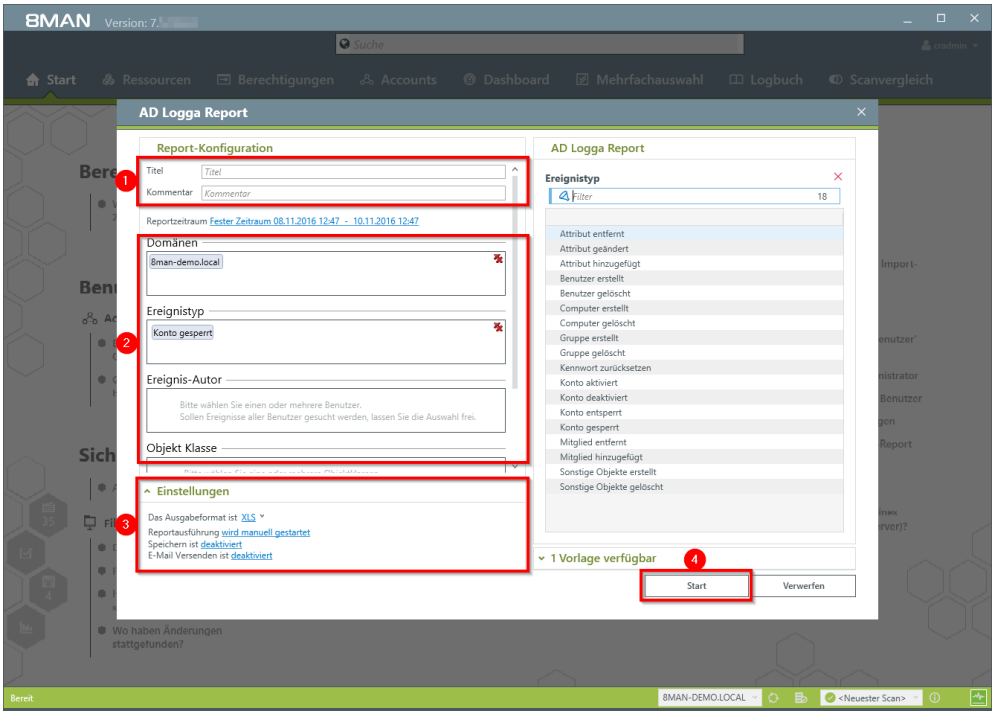
Weiterführende Services

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

Der Prozess in einzelnen Schritten



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



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

5.4 Kennwortzurücksetzungen überwachen

Hintergrund / Mehrwert

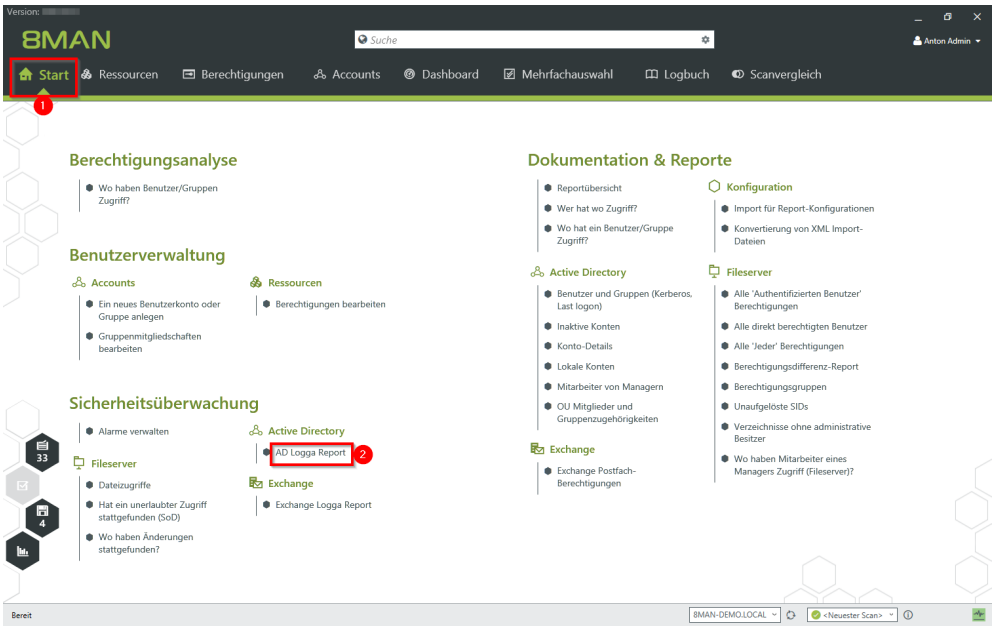
Mit dem 8MATE AD Logga überwachen Sie den Prozess des Kennwortrücksetzens. Diesem ist ein Sicherheitsrisiko inhärent. Setzt beispielsweise ein Helpdesk-Mitarbeiter heimlich das Kennwort einer Führungskraft zurück, kann er mit dem Übergangspasswort sich anmelden und geheime Daten einsehen. Die betroffene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

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

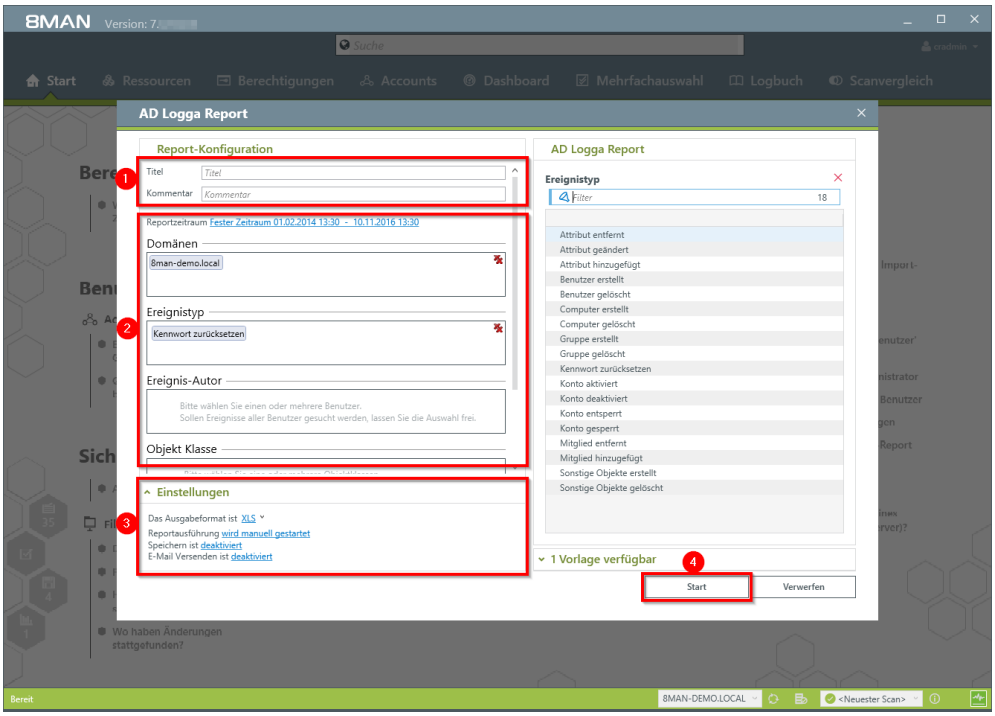
Weiterführende Services

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

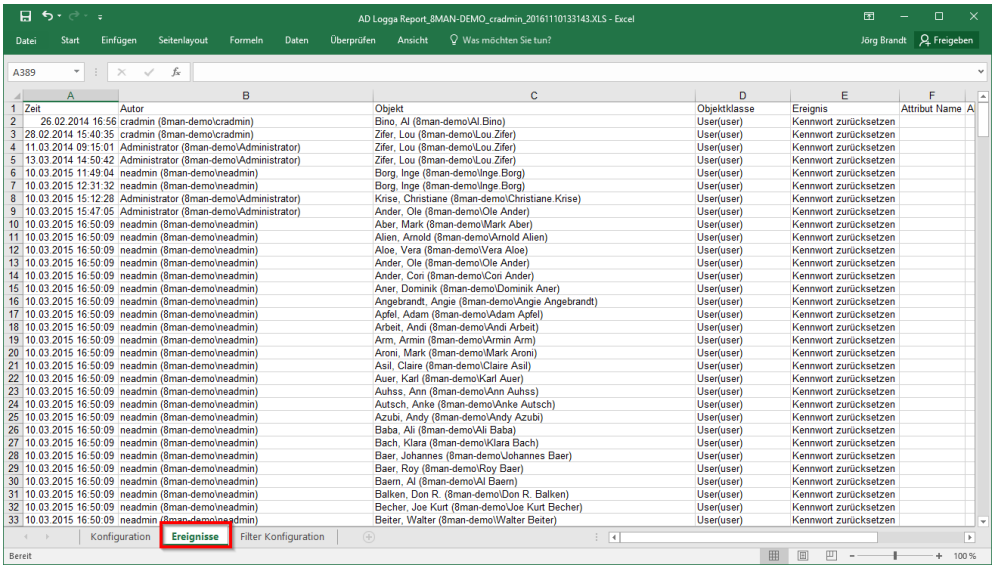
Der Prozess in einzelnen Schritten



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



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



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

5.5 AD Logga Ereignisse mit dem Logbuch auswerten

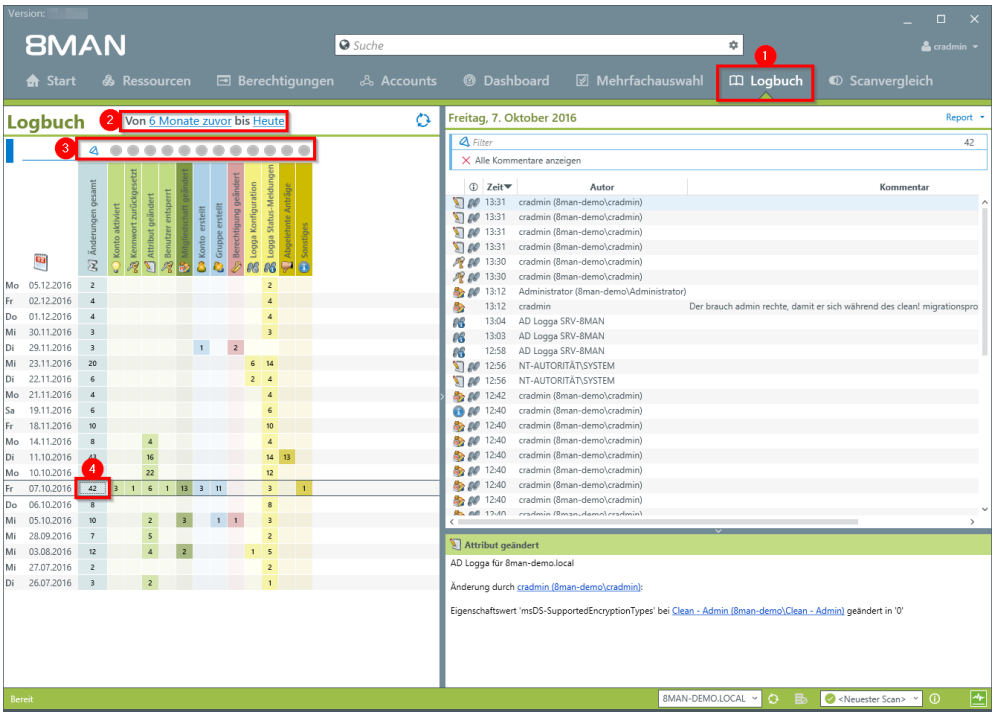
Hintergrund / Mehrwert

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

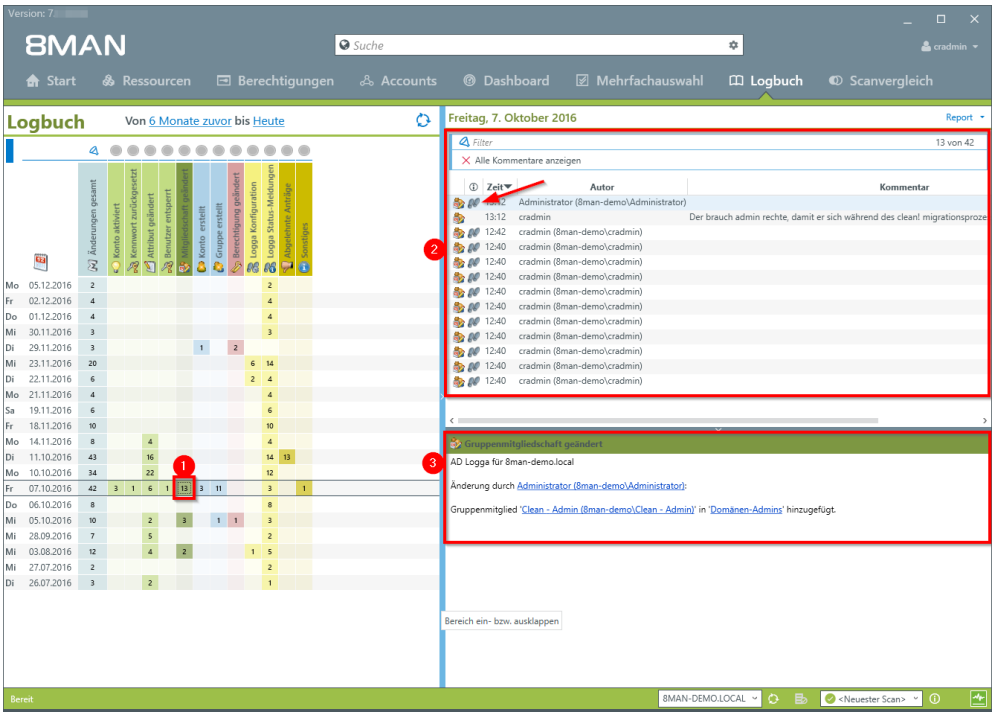
Weiterführende Services

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

Der Prozess in einzelnen Schritten



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



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

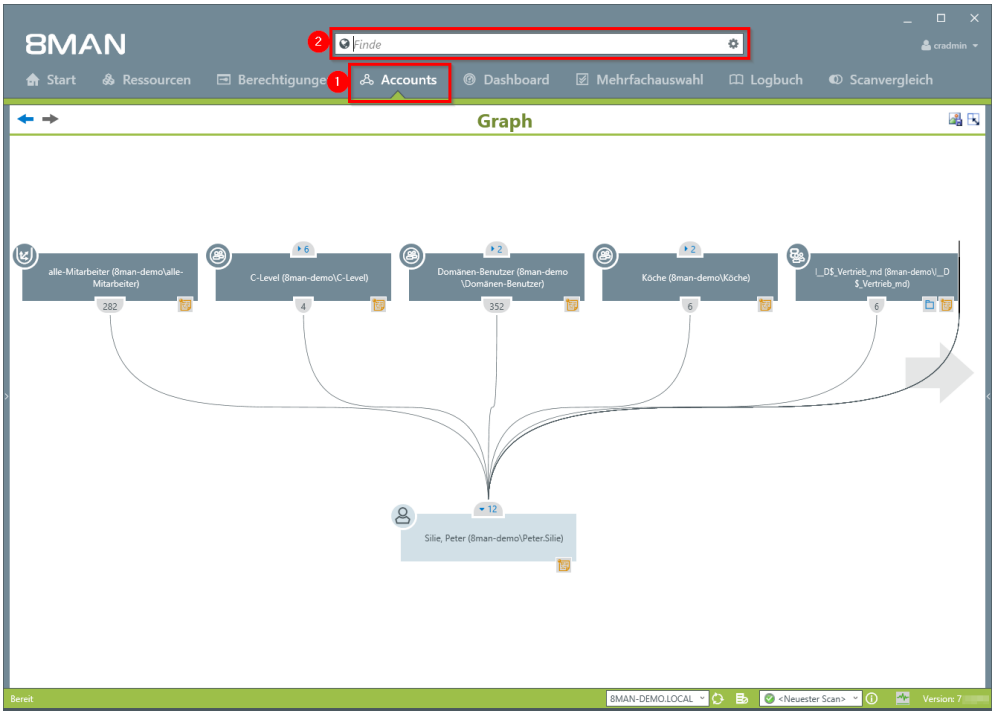
5.6 Die letzten Aktionen an einem Nutzerkonto oder einer AD Gruppe identifizieren

Hintergrund / Mehrwert

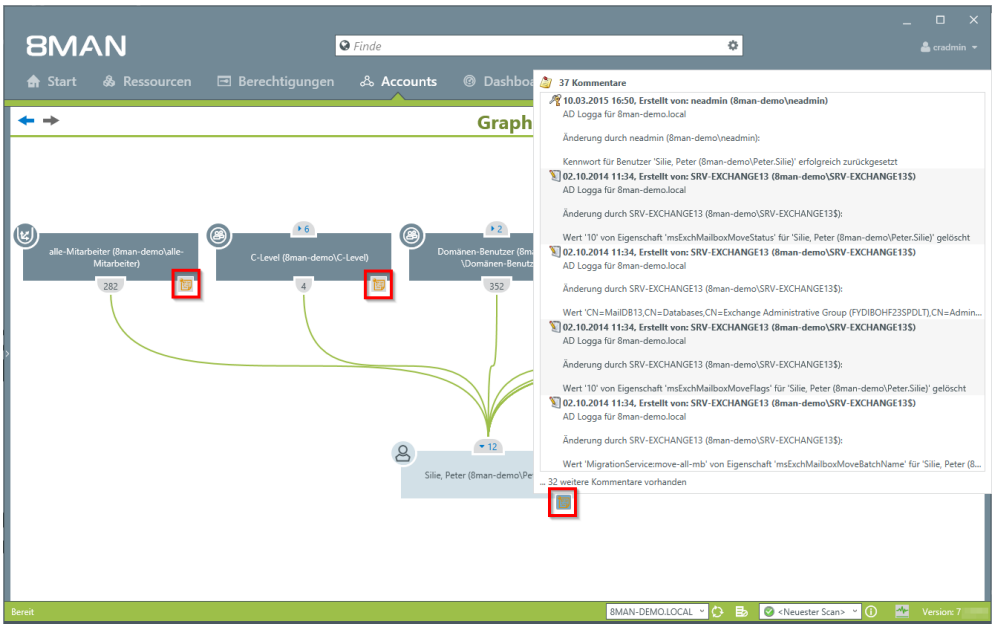
Nutzerkonten und Gruppen haben eine eigene Historie. Deshalb macht es Sinn, vor der weiteren Bearbeitung zu prüfen, was vorher durchgeführte Aktivitäten waren.

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

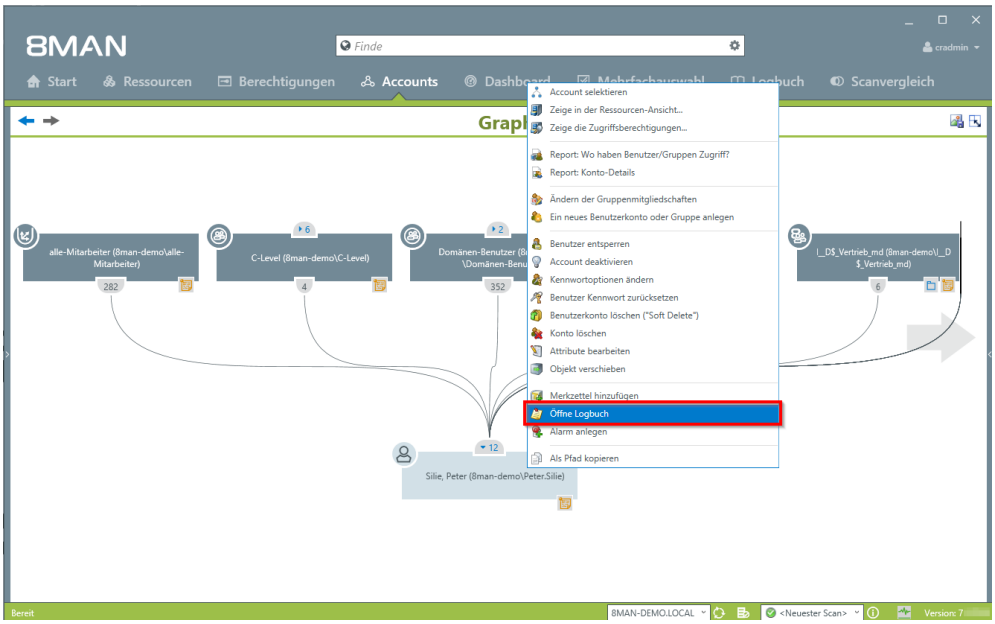
Der Prozess in einzelnen Schritten



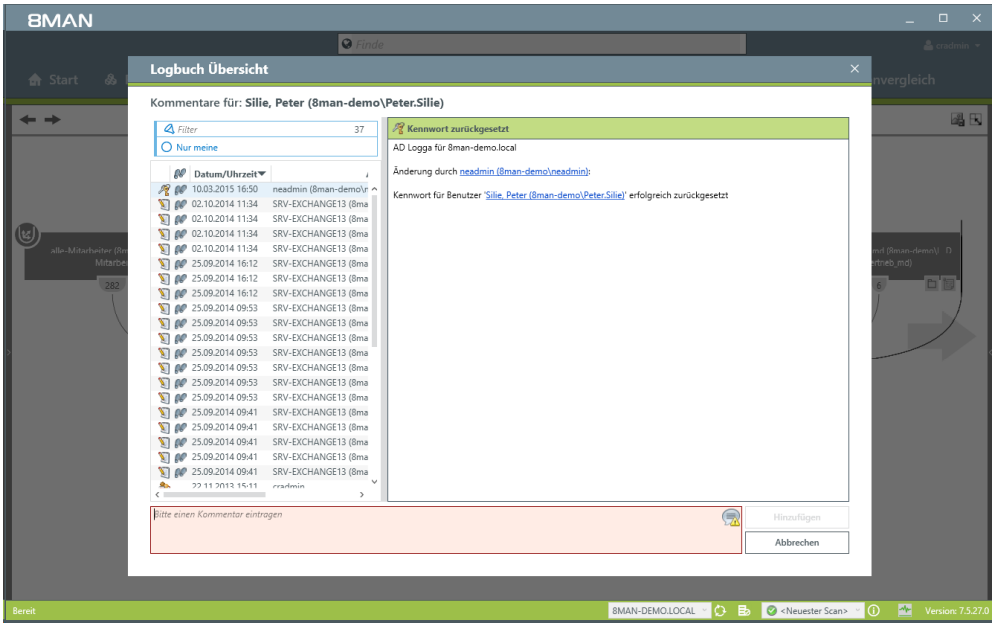
1. *Wählen Sie "Accounts".*
2. *Suchen Sie nach dem gewünschten Nutzer oder der gewünschten Gruppe.*



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

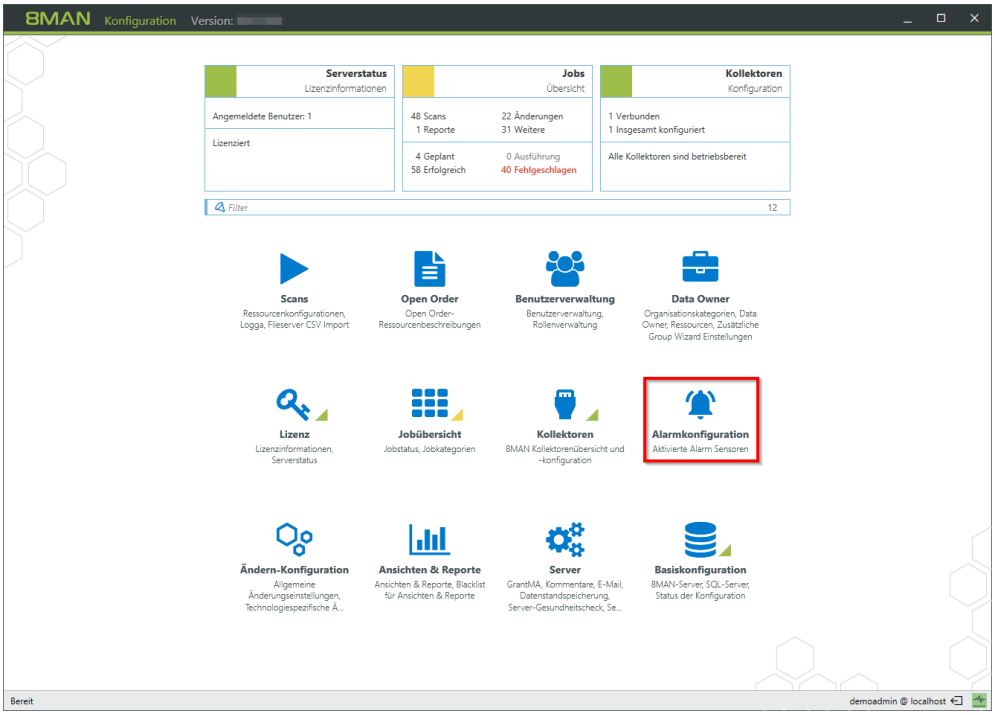


Klicken Sie mit rechts auf das gewünschte Objekt und wählen dann "Öffne Logbuch", um alle aufgezeichneten Informationen zu erhalten.



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

6 Alarme konfigurieren



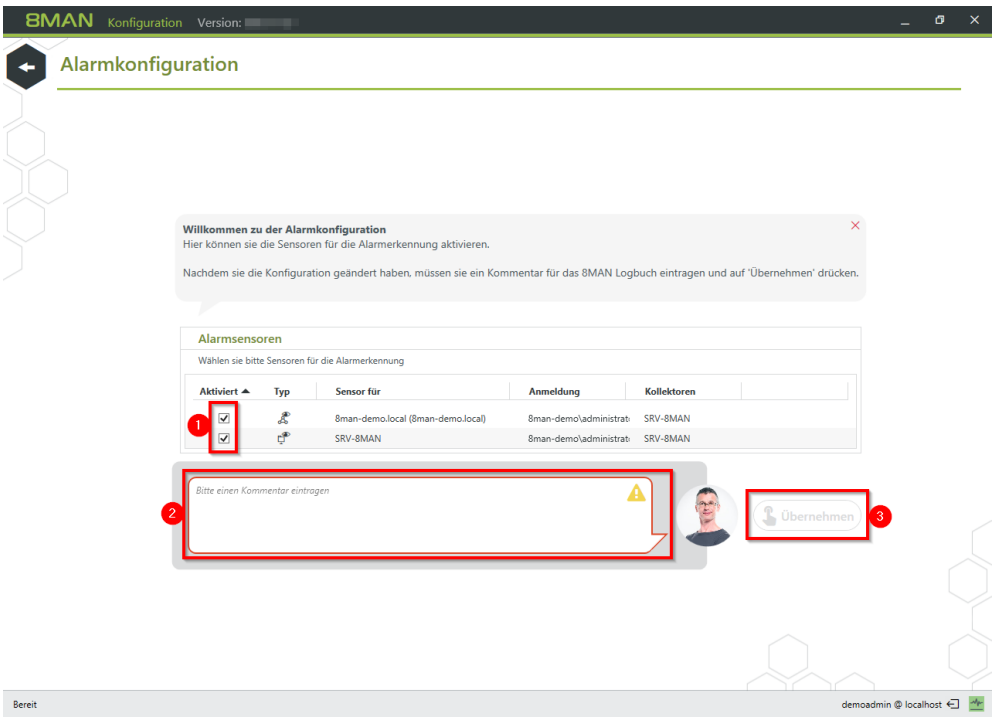
In der Kategorie "Alarme" aktivieren und deaktivieren Sie die Alarm-Sensoren.

Mit aktiven Alarmsensoren können Sie Alarme für Gruppen oder Nutzerkonten anlegen.

In der 8MAN Benutzeroberfläche verwalten Sie angelegte Alarme.

Sie benötigen eine Lizenz für die 8MATEs FS Logga oder AD Logga.

6.1 AD-Logga Alarmsensoren aktivieren/deaktivieren



1. *Aktivieren/Deaktivieren Sie die Alarmsensoren.*
2. *Sie müssen einen Kommentar angeben.*
3. *Übernehmen Sie die Einstellungen.*

Nur mit aktiven Alarmsensoren sind die Alarmkonfigurationen wirksam.

6.2 Alarme für Gruppen anlegen

Hintergrund / Mehrwert

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

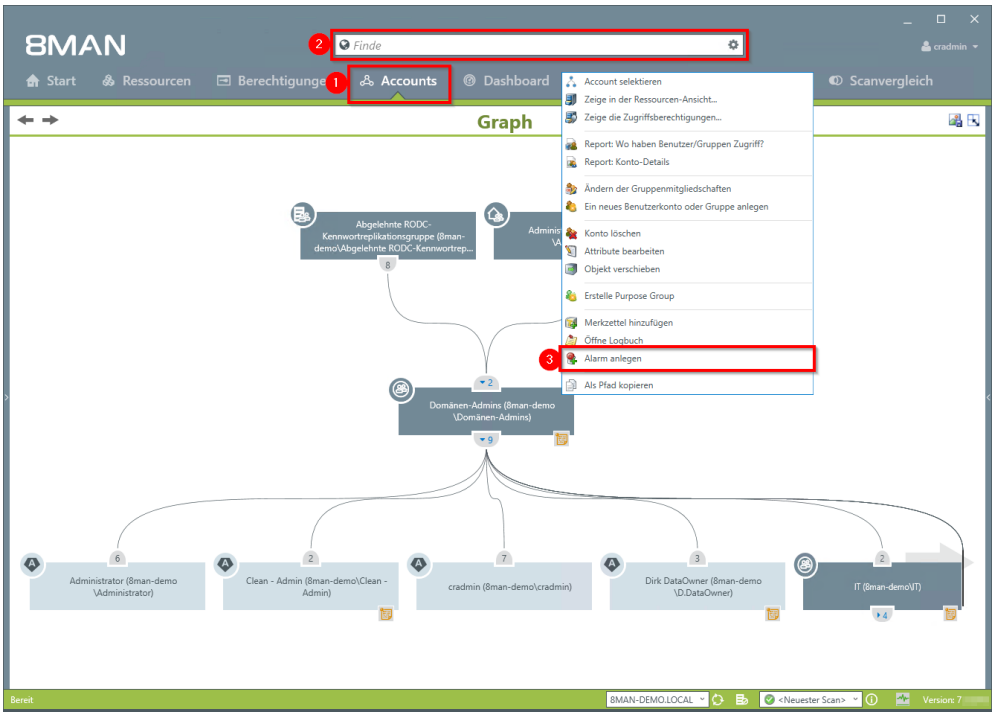
Die Gruppenverschachtelungen im Active Directory machen es notwendig, auch Gruppenmitgliedschaften zu überwachen, die sich aus neuen, indirekten Mitgliedschaften ergeben. Ein Beispiel: Die Gruppe „Geschäftsführer“ wird überwacht und hat als Mitglied die Gruppe „geheime Daten“. 8MATE AD Logga Alarme benachrichtigen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

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

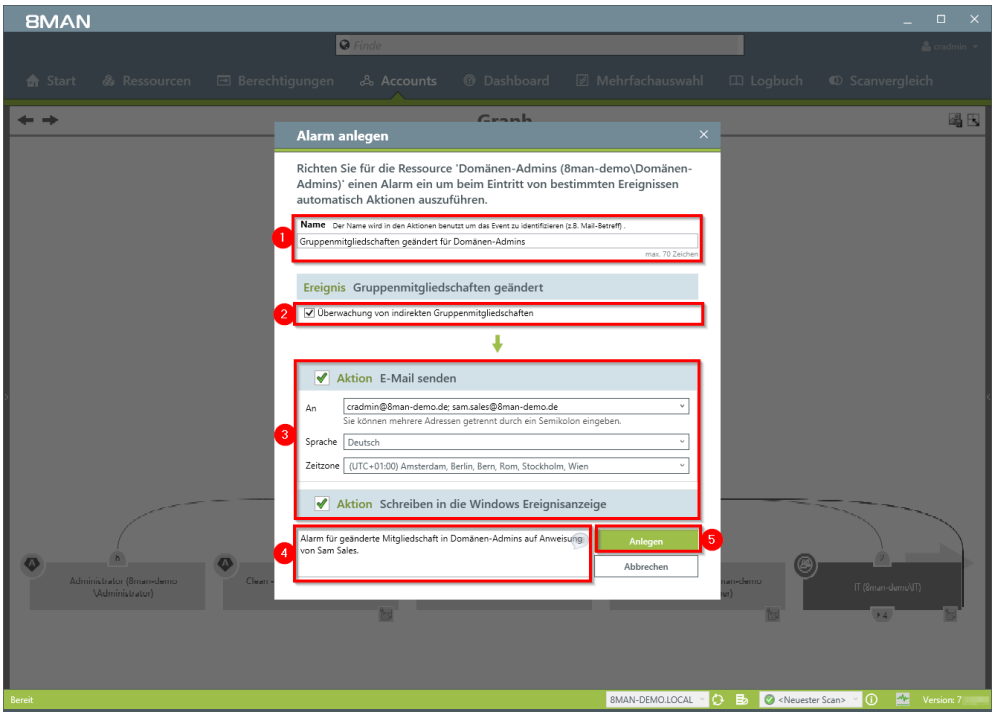
Weiterführende Services

Alarmsensoren aktivieren/deaktivieren
Alarme für Nutzerkonten anlegen
Alarme verwalten

Der Prozess in einzelnen Schritten



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



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

6.3 Alarme für Nutzerkonten anlegen

Hintergrund / Mehrwert

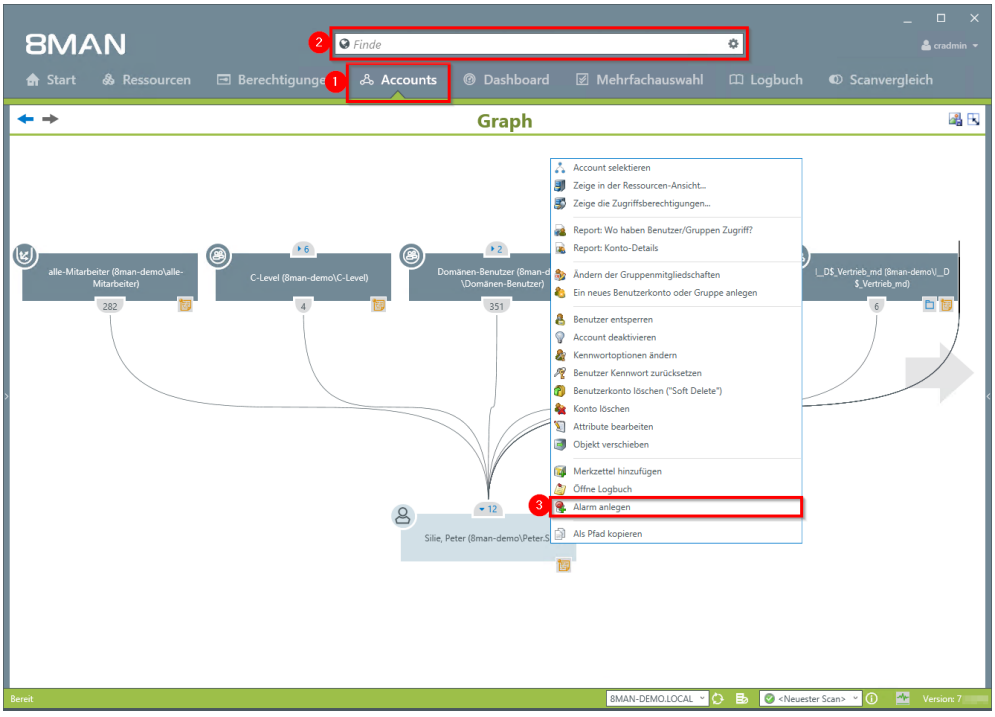
Mit dem 8MATE AD Logga überwachen Sie den Prozess des Kennwortrücksetzens. Diesem ist ein Sicherheitsrisiko inhärent. Setzt beispielsweise ein Helpdesk-Mitarbeiter heimlich das Passwort einer Führungskraft zurück, kann er mit dem Übergangspasswort sich anmelden und geheime Daten einsehen. In diesem Fall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

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

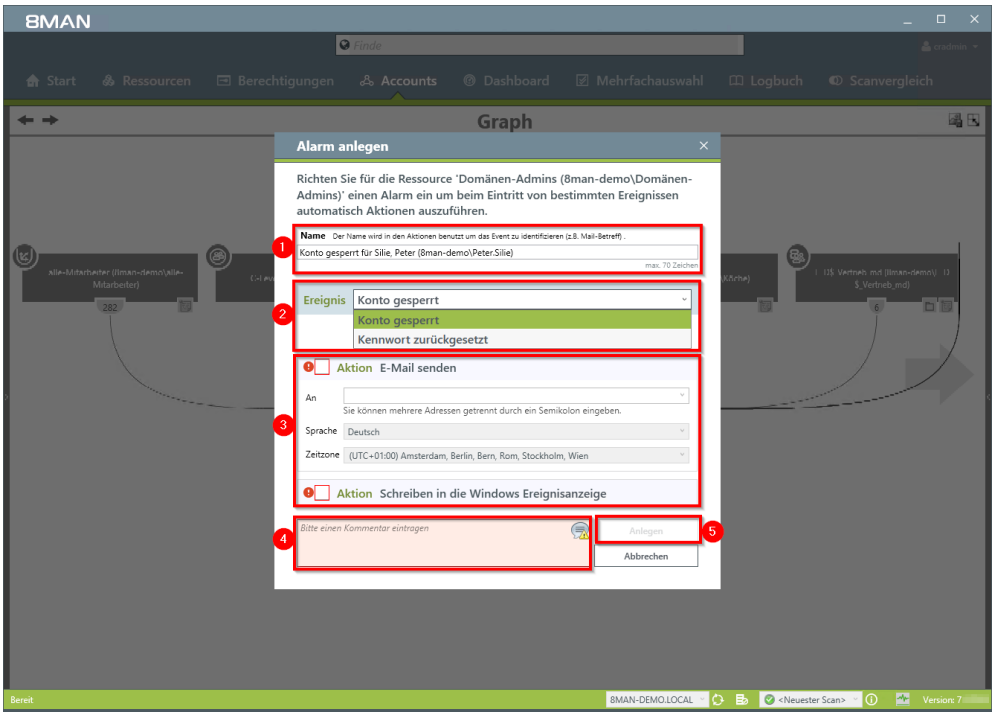
Weiterführende Services

Alarmsensoren aktivieren/deaktivieren
Alarme für Gruppen anlegen

Der Prozess in einzelnen Schritten



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



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

6.4 Alarme verwalten

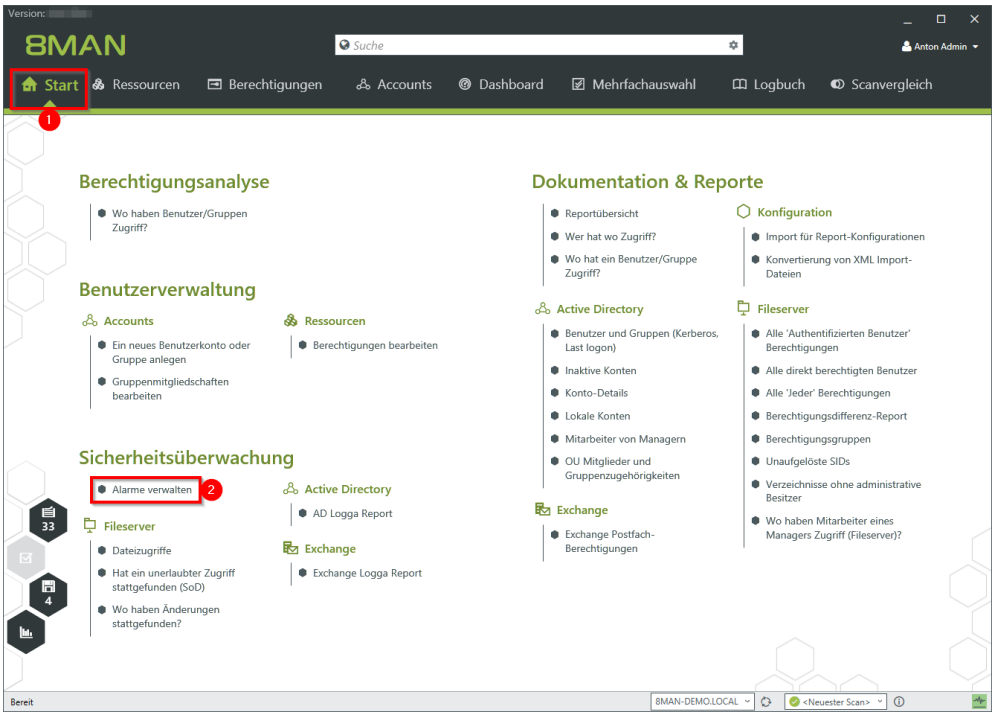
Hintergrund / Mehrwert

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

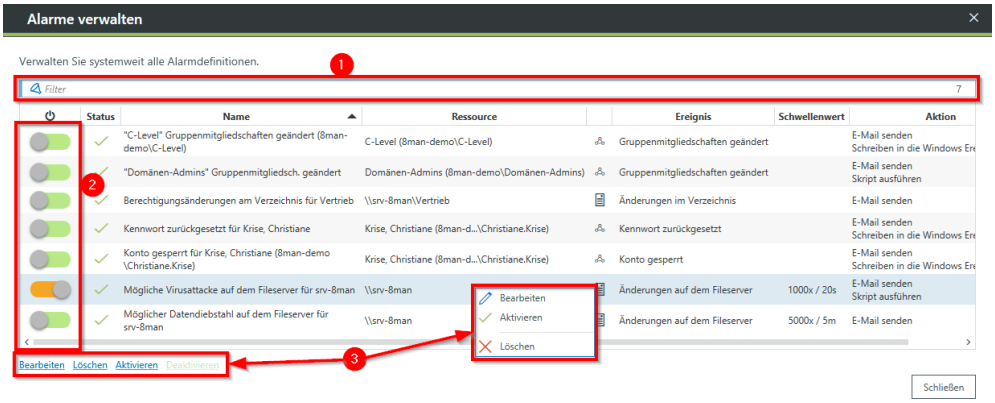
Weiterführende Services

Alarmsensoren aktivieren/deaktivieren

Der Prozess in einzelnen Schritten



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



8MAN zeigt Ihnen alle Alarmkonfigurationen.

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

7 Den 8MAN Support kontaktieren

Sie erreichen unseren Support

per Telefon
+49 30 390 6345-99
Montag bis Freitag von 9.00 bis 17.00 Uhr.

per E-Mail
support@8man.com

per Website
https://susi.8man.com

Sie starten auf der Website mit einer Selbstregistrierung. Nach Abschluss können Sie die öffentlich zugänglichen Inhalte sehen.
Nach der Registrierung werden Sie durch unseren Support einer Berechtigungsebene zugeordnet. Erst dann können Sie nicht-öffentliche Inhalte sehen und das Ticketsystem nutzen.
Dieser Vorgang kann etwas Zeit in Anspruch nehmen.

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
- WpfAnimatedGif, © Copyright 2012-2017 Thomas Levesque, https://github.com/XamlAnimatedGif/WpfAnimatedGif/blob/master/LICENSE.txt
- Bootstrap, © 2011-2016 Twitter, Inc, https://github.com/twbs/bootstrap/blob/master/LICENSE
- jQuery, © 2016 The jQuery Foundation, https://jquery.org/license
- jquery.cookie, © 2014 Klaus Hartl, https://github.com/carhartl/jquery-cookie/blob/master/MIT-LICENSE.txt
- jquery-tablesort, © 2013 Kyle Fox, https://github.com/kylefox/jquery-tablesort/blob/master/LICENSE
- LoadingDots, © 2011 John Nelson, http://johncoder.com
- easyModal.js, © 2012 Flavius Matis, https://github.com/flaviusmatis/easyModal.js/blob/master/LICENSE.txt
- jsTimezoneDetect, © 2012 Jon Nylander https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENCE.txt?at=defaultjquery-tablesort
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community https://github.com/janl/mustache.js/blob/master/LICENSE
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE
- Underscore.js, © 2009-2016 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors https://github.com/jashkenas/underscore/blob/master/LICENSE
- Ractive.js, © 2012-15 Rich Harris and contributors, https://github.com/ractivejs/ractive/blob/dev/LICENSE.md
- RequireJS, © 2010-2015, The Dojo Foundation, https://github.com/jrburke/requirejs/blob/master/LICENSE
- typeahead.js, © 2013-2014 Twitter, Inc, https://github.com/twitter/typeahead.js/blob/master/LICENSE
- Select2, © 2012-2015 Kevin Brown, Igor Vaynberg, and Select2 contributors https://github.com/select2/select2/blob/master/LICENSE.md
- bootstrap-datepicker, © Copyright 2013 eternicode https://github.com/eternicode/bootstrap-datepicker/blob/master/LICENSE
- RabbitMQ, © Copyright 2007-2013 GoPivotal, https://www.rabbitmq.com/mpl.html

- EPPlus, JanKallman, https://github.com/JanKallman/EPPlus/blob/master/LICENSE