Identity Console
Administrationshandbuch

September 2022

Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch und zur Bibliothek

Das *Administrationshandbuch* enthält grundlegende Informationen zum Konzept von NetIQ Identity Console (Identity Console). Dieses Handbuch enthält Terminologiedefinitionen und beschreibt Implementierungsszenarien.

Die neueste Version des *NetIQ Identity Console-Administrationshandbuchs* finden Sie in der englischen Version der Dokumentation auf der NetIQ Identity Console-Onlinedokumentations-Website.

Zielgruppe

Dieses Handbuch richtet sich an Netzwerkadministratoren.

Weitere Informationen in der Bibliothek

Die Bibliothek enthält folgende Informationsressourcen:

Installationsanleitung

Beschreibt die Installation von Identity Console. Dieses Handbuch richtet sich an Netzwerkadministratoren.

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Fokus liegt auf drei besonderen Herausforderungen, die Sie in Ihrer Umgebung meistern müssen: Änderungen, Komplexität und Risiken. Unser Ziel ist es, Sie dabei zu unterstützen.

Unser Standpunkt

Sich an Änderungen anzupassen und Komplexität und Risiken zu beherrschen ist nichts Neues

Unter den verschiedenen Herausforderungen, denen Sie gegenüberstehen, beeinflussen diese drei Punkte sicherlich am meisten Ihre Möglichkeiten, Ihre physischen, virtuellen und Cloud-Umgebungen sicher zu messen, zu überwachen und zu verwalten.

Kritische Geschäftsservices schneller und besser bereitstellen

Wir sind davon überzeugt, dass IT-Organisationen über eine möglichst umfassende Kontrolle verfügen müssen, um eine zeitgerechte und kostenwirksame Servicebereitstellung zu ermöglichen. Der von Änderungen und Komplexität ausgehende, kontinuierliche Druck steigt ständig, weil sich die Unternehmen ständig ändern und die erforderlichen Technologien zur Verwaltung der Änderungen immer komplexer werden.

Unsere Philosophie

Intelligente Lösungen entwickeln, nicht einfach Software

Um zuverlässige Lösungen für die Kontrolle anbieten zu können, stellen wir erst einmal sicher, dass wir die Szenarien, in dem Unternehmen wie das Ihre täglich arbeiten, gründlich verstehen. Nur so können wir praxistaugliche, intelligente IT-Lösungen entwickeln, die nachweisbar messbare Ergebnisse liefern. Und das ist für uns wesentlich bereichernder, als einfach eine Software zu verkaufen.

Ihr Erfolg ist unsere Leidenschaft

Ihr Erfolg ist der Wegweiser für unser Geschäft. Wir wissen, dass Sie von der Produktkonzeption bis hin zur Bereitstellung IT-Lösungen benötigen, die richtig funktionieren und nahtlos mit Ihren vorhandenen Investitionen integriert werden können. Sie benötigen fortlaufenden Support, Schulungen nach der Bereitstellung und jemanden, mit dem Sie unkompliziert arbeiten können. Ihr Erfolg ist auch unser Erfolg.

Unsere Lösungen

- Identitäts- und Zugriffsregelung
- Zugriffsverwaltung
- Sicherheitsverwaltung

- System- und Anwendungsverwaltung
- Workload-Management
- Serviceverwaltung

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen, wenden Sie sich an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Wenn Sie uns einen Verbesserungsvorschlag mitteilen möchten, nutzen Sie die Schaltfläche **Comment on this topic** (Ihr Kommentar zu diesem Thema), die unten auf jeder Seite der unter www.netiq.com/documentation veröffentlichten HTML-Versionen unserer Dokumentation verfügbar ist. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

Qmunity, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. Qmunity bietet Ihnen aktuellste Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über alle Voraussetzungen verfügen, um das meiste aus den IT-Investitionen zu holen, auf die Sie sich verlassen. Weitere Informationen hierzu finden Sie im Internet unter http://community.netiq.com.

1 Was ist Identity Console?

Identity Console ist eine moderne, webbasierte Administrationskonsole, mit der Sie über das Internet und einen Webbrowser von einem beliebigen Standort aus auf virtuelle, sichere und benutzerdefinierte Weise auf Netzwerkadministrationsprogramme zugreifen können. Identity Console erleichtert die dezentrale Bearbeitung von Administrationsaufgaben.

Funktionen von Identity Console

Identity Console bietet die folgenden Funktionen:

- Verwalten von eDirectory-Objekten, -Benutzern, -Schemas, -Partitionen, -Replikaten, -Rechten usw.
- Verwalten von Identity Manager-Treibern und Treibersätzen
- Verwalten und Anzeigen von Treiberleistungsstatistiken
- Überprüfen von Objekten, Anzeigen des Datenflusses von Treibern, Verwalten von Berechtigungen, Arbeitsaufträgen usw.
- Verwalten des Passwortsynchronisierungsstatus und der Einstellungen für Treiber
- Verwalten von Passwortrichtlinien und Anmeldemethoden
- Zertifikate verwalten
- Verwalten verschiedener Netzwerkressourcen
- Bessere Sicherheitsmaßnahmen zum Schutz Ihrer Daten
- Bessere Skalierbarkeit zum Verwalten größerer eDirectory-Objekte
- Sichere Anmeldung am Identity Console-Portal über One SSO Provider (OSP)
- Modernste Benutzeroberflächentechnologie
- Einfache Installation und Konfiguration über Docker-Container

2 Zugriff auf Identity Console

Der Zugriff auf Identity Console und die gesamte Funktionalität der Lösung ist über jeden unterstützten Webbrowser möglich. Zwar können Sie möglicherweise auch über einen nicht in der Liste enthaltenen Webbrowser auf Identity Console zugreifen, die vollständige Funktionalität und Unterstützung wird jedoch nur für die offiziell unterstützten Browser gewährleistet.

WICHTIG: Informationen zu unterstützten Webbrowsern finden Sie im *Identity Console-Installationshandbuch*.

Auf Identity Console zugreifen

Führen Sie die folgenden Schritte aus, um auf die serverbasierte Instanz von Identity Console zuzugreifen:

1. Geben Sie in das Adressfeld (URL-Feld) eines unterstützten Webbrowsers Folgendes ein:

   Sichere Anmeldung: `https://<Server-IP-Adresse/Hostname>:<Port>/identityconsole/`

   Die IP-Adresse, die in den Beispielen als *<Server-IP-Adresse>* angegeben ist, muss eine IPv4-Adresse sein. Der standardmäßige Port ist 9000.
2. Melden Sie sich mit Ihrem Benutzer-DN und Passwort an.
3. Geben Sie die IP-Adresse oder den DNS-Namen für den eDirectory-Baum mit oder ohne sicheren LDAP-Port an.

HINWEIS

- Das Aktualisieren einer beliebigen Registerkarte in Identity Console führt aus Sicherheitsgründen zur Abmeldung des Benutzers.
- Das Öffnen doppelter Identity Console-Registerkarten im Browser führt aus Sicherheitsgründen zur Abmeldung des Benutzers.
- Der DN sollte im Format `cn=admin,ou=sa,o=system` angegeben werden.
- Wenn eDirectory mit einem nicht standardmäßigen Port konfiguriert ist, müssen Sie die Portnummer angeben.

---

3 In der Identity Console-Benutzeroberfläche navigieren

Dieser Abschnitt beschreibt das Navigieren in der Identity Console-Weboberfläche.

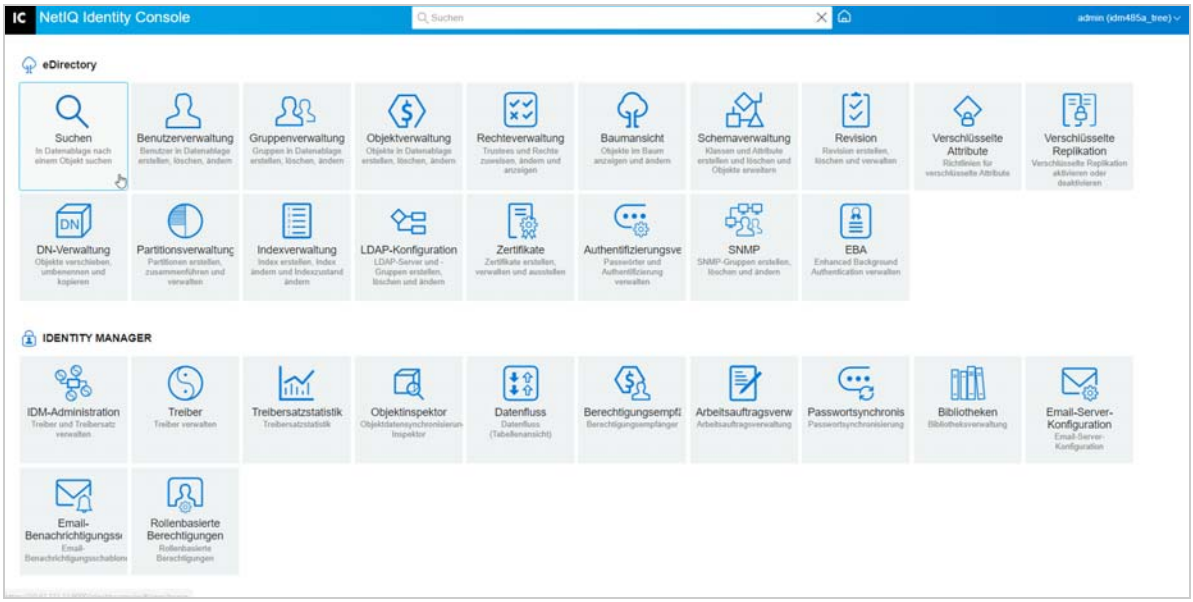
Suche (Technologievorschau)

Die Funktion **Suche (Technologievorschau)** stellt ein Ausgangslayout für die Suchfunktion bereit. In dieser Vorschau können Sie Schlüsselwörter angeben und das Suchfeld bestimmt die Informationsquelle, um übereinstimmende Ergebnisse zu suchen und anzuzeigen. Mit dieser Option können Sie nach einer Ressource suchen und auf jeder Seite der Identity Console-Anwendung problemlos darauf zugreifen.

Identity Console-Benutzeroberfläche

Die Identity Console-Benutzeroberfläche umfasst die eDirectory- und Identity Manager-Module.

Abbildung 3-1 *Identity Console-Benutzeroberfläche*



WICHTIG: Bestimmte GIF-Animationen in diesem Handbuch funktionieren nur in der Online-Dokumentation. Falls Sie die PDF-Version verwenden, sind nur Screenshots sichtbar.

Tabelle 3-1 *Erläuterung verschiedener Module des Identity Console-Webportals*

Modulname	Beschreibung
Suche	Objekt in der Datenablage suchen. Weitere Informationen finden Sie in Kapitel 4, „Suchen ausführen“, auf Seite 23.
Benutzerverwaltung	Benutzer in der Datenablage erstellen, löschen und ändern. Weitere Informationen finden Sie im Kapitel 5, „Benutzer verwalten“, auf Seite 27.
Gruppenverwaltung	Gruppen in der Datenablage erstellen, löschen und ändern. Weitere Informationen finden Sie unter Kapitel 6, „Gruppen verwalten“, auf Seite 35.
Objektverwaltung	Objekte in der Datenablage erstellen, löschen und ändern. Weitere Informationen finden Sie in Kapitel 7, „Objekte verwalten“, auf Seite 41.
Rechteverwaltung	Trustees und Rechte zuweisen, ändern und anzeigen. Weitere Informationen finden Sie in Kapitel 8, „Rechte verwalten“, auf Seite 49.
Baumansicht	Objekte im Baum anzeigen und ändern. Weitere Informationen finden Sie im Kapitel 9, „Baumansicht“, auf Seite 53.
Schemaverwaltung	Klassen, Zusatzklassen und Attribute erstellen und löschen und Objekte erweitern. Weitere Informationen finden Sie in Kapitel 10, „Schema verwalten“, auf Seite 57.
Revision	CEF-Revision aktivieren, deaktivieren und verwalten. Weitere Informationen finden Sie im Kapitel 11, „Revisionsereignisse verwalten“, auf Seite 65.
Verschlüsselte Attribute	Richtlinie für verschlüsselte Attribute erstellen, ändern, löschen und anzeigen. Weitere Informationen finden Sie im Kapitel 12, „Verschlüsselte Attribute verwalten“, auf Seite 71.
Verschlüsselte Replikation	Verschlüsselte Replikation aktivieren, deaktivieren und anzeigen. Weitere Informationen finden Sie in Kapitel 13, „Verschlüsselte Replikation verwalten“, auf Seite 75.
DN-Verwaltung	Objekte verschieben, umbenennen und kopieren. Weitere Informationen finden Sie im Kapitel 7, „Objekte verwalten“, auf Seite 41.
Verwaltung von Partitionen	Partitionen und Replikate erstellen, zusammenführen und verschieben. Weitere Informationen finden Sie im Kapitel 14, „Partitionen und Reproduktionen verwalten“, auf Seite 77.
Indexverwaltung	Indizes erstellen und ändern und den Indexstatus ändern. Weitere Informationen finden Sie im Kapitel 15, „Indizes verwalten“, auf Seite 83.

Modulname	Beschreibung
LDAP-Konfiguration	LDAP-Objekte erstellen, löschen und ändern. Weitere Informationen finden Sie im Kapitel 16, „LDAP-Objekte konfigurieren“, auf Seite 87.
Zertifikatsverwaltung	Server- und Zertifizierungsstellenzertifikaten erstellen und verwalten. Weitere Informationen finden Sie in Kapitel 17, „Zertifikate verwalten“, auf Seite 91.
Authentifizierungsverwaltung	Anmeldemethoden, Anmeldefolgemethoden und Anmeldemethodensequenzen erstellen und verwalten. Mit diesem Modul können Sie auch Passwortrichtlinien und Sicherheitsabfragensätze verwalten. Weitere Informationen finden Sie im Kapitel 18, „Authentifizierungs-Framework verwalten“, auf Seite 111.
SNMP	SNMP-Gruppen erstellen, löschen und ändern. Weitere Informationen finden Sie im Kapitel 19, „SNMP-Gruppenobjekte verwalten“, auf Seite 127.
EBA	Enhanced Background Authentication verwalten. Weitere Informationen finden Sie im Kapitel 20, „Enhanced Background Authentication verwalten“, auf Seite 131.
IDM-Verwaltung	Identity Manager-Treiber und Treibersätze verwalten. Weitere Informationen finden Sie im Kapitel 21, „Treiber und Treibersätze verwalten“, auf Seite 135. Mit diesem Modul können Sie auch die Treibersatzeigenschaften verwalten. Weitere Informationen finden Sie im Kapitel 22, „Treibersatzeigenschaften verwalten“, auf Seite 141.
Treibereigenschaften	Die Eigenschaften verschiedener Treiber verwalten. Weitere Informationen finden Sie im Kapitel 23, „Treibereigenschaften verwalten“, auf Seite 155.
Treibersatzstatistiken	Treibersatzstatistiken anzeigen und verwalten. Weitere Informationen finden Sie unter Kapitel 24, „Treibersatzstatistiken verwalten“, auf Seite 187.
Objekt inspektor	Objektverknüpfung und Datensynchronisierung verwalten. Weitere Informationen finden Sie im Kapitel 25, „Identity Manager-Objekte untersuchen“, auf Seite 189.
Datenfluss	Datenfluss der Treiber verwalten und anzeigen. Weitere Informationen finden Sie im Kapitel 26, „Datenfluss verwalten“, auf Seite 191.
Berechtigungsempfänger	Berechtigungsempfänger verwalten. Weitere Informationen finden Sie im Kapitel 27, „Berechtigungsempfänger verwalten“, auf Seite 193.

Modulname	Beschreibung
Arbeitsauftragsverwaltung	Arbeitsaufträge verwalten. Weitere Informationen finden Sie im Kapitel 28, „Arbeitsaufträge verwalten“, auf Seite 195.
Passwortsynchronisierung	Passwortsynchronisierung und Passwortsynchronisierungsstatus verwalten. Weitere Informationen finden Sie im Kapitel 29, „Passwortstatus und Passwortsynchronisierung verwalten“, auf Seite 199.
Bibliotheksverwaltung	Bibliotheken verwalten. Weitere Informationen finden Sie unter Kapitel 30, „Bibliotheken verwalten“, auf Seite 203.
Email-Server-Konfiguration	Optionen für den Email-Server verwalten. Weitere Informationen finden Sie unter Kapitel 31, „Email-Serveroptionen verwalten“, auf Seite 205.
Email-Benachrichtigungsschablonen	Email-Schablonen verwalten. Weitere Informationen finden Sie unter Kapitel 32, „Email-Schablonen verwalten“, auf Seite 207.

Verwalten von eDirectory mit Identity Console

In diesem Abschnitt werden verschiedene Aufgaben beschrieben, mit denen Sie Ihre(n) eDirectory-Server mithilfe des Identity Console-Portals verwalten können.

4 Suchen ausführen

Auf der Suchkachel können Sie eine Suchoperation angeben, die im Verzeichnisbaum ausgeführt werden soll, und die Ergebnisse anzeigen. Mit dieser Option können Sie nach verschiedenen Objekten, Benutzern, Gruppen usw. suchen. Führen Sie die unten aufgeführten Schritte aus, um nach verschiedenen Objekten in der Datenablage zu suchen:

1. Geben Sie den Objektnamen für die Suche an. Verwenden Sie ein Sternchen (*) als Platzhalter, um einen unvollständigen Namen anzugeben. Beispiel: `ldap*`, `*zert`, `*server*` usw. Wenn Sie in dieses Feld nur ein Sternchen eingeben, gibt Identity Console alle Suchergebnisse für den ausgewählten **Typ** und **Kontext** zurück.

   HINWEIS: Mit dem Kontextbrowser können Sie den gesamten eDirectory-Baum durchsuchen, indem Sie im Suchfeld ein Sternchen (*) angeben. Sie können die Objekte im Kontextbrowser auch mithilfe der Platzhaltersuche filtern. Beispiel: `admin*`. Dieses Verhalten des Kontextbrowsers wird in verschiedenen Modulen in Identity Console unterstützt.

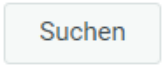
   ---

2. Wählen Sie den Objekttyp für die Suche im Feld **Typ** aus. Identity Console zeigt nur Objekte des angegebenen Typs an. Standardmäßig ist in diesem Feld der Typ **Benutzer** ausgewählt.

   Klicken Sie auf das Symbol  , um zusätzliche Sucheinstellungen auf Attributebene zu definieren. Weitere Informationen finden Sie unter „Erweiterte Suche konfigurieren“, auf Seite 24.

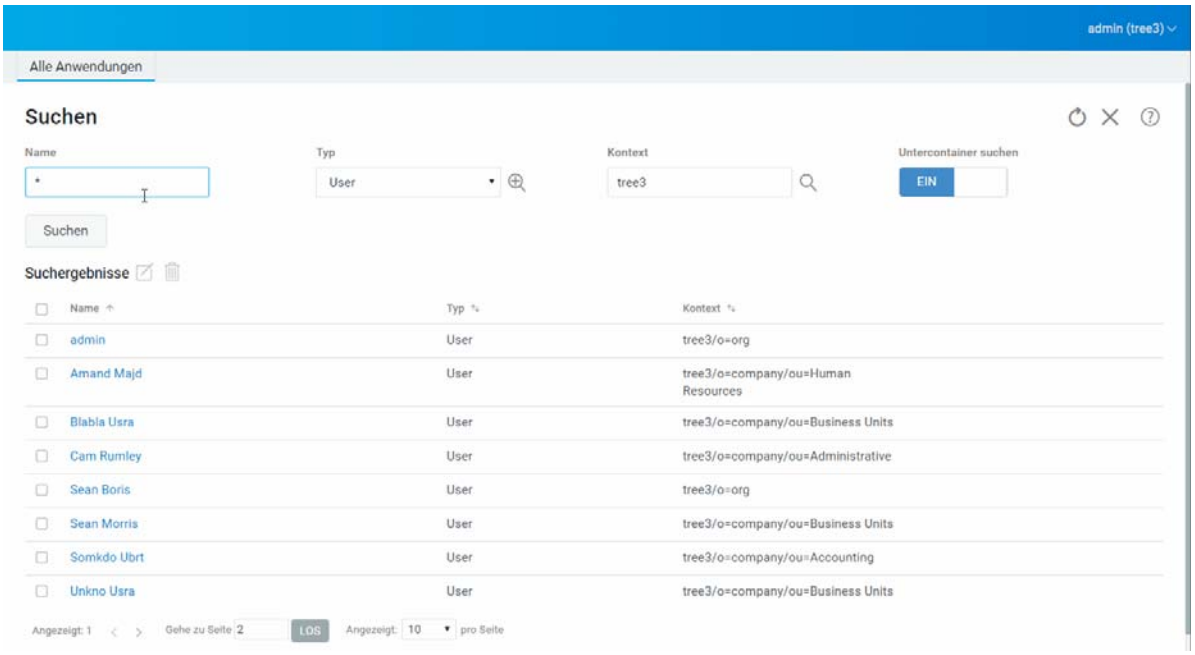
3. Geben Sie den Anfangscontainer für die Suchoperation im Feld **Kontext** an.

4. Wenn untergeordnete Container in die Suche einbezogen werden sollen, setzen Sie die Option zum Durchsuchen von Untercontainern auf **EIN**.

5. Klicken Sie auf die Schaltfläche 

.

Abbildung 4-1 *Ausführen einer Suchoperation*



Erweiterte Suche konfigurieren

Die Funktion der erweiterten Auswahl bietet eine besser konfigurierbare Umgebung für die Suche nach gewünschten Objekten im Verzeichnis.

Objekttyp: Legt die Basis-Objektklasse fest, nach der Sie suchen. Beispiel: "Benutzer".

Zusatzklassen: Klicken Sie auf das Symbol +, um eine Zusatzklasse anzugeben, die in die Suche einbezogen werden soll.

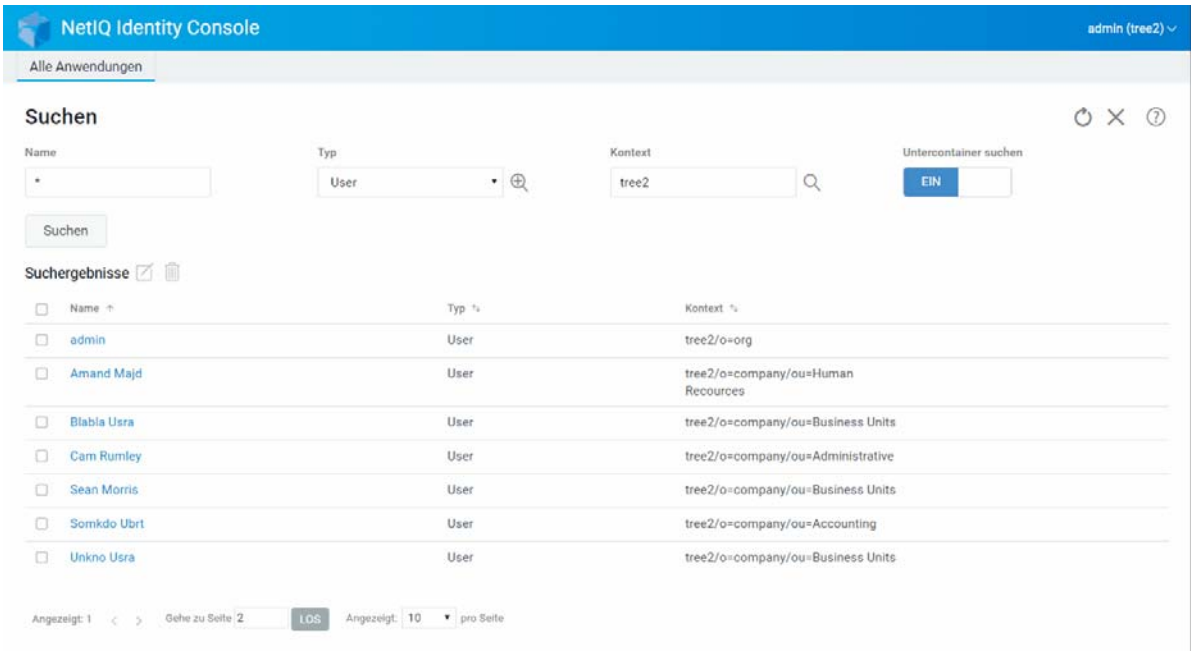
Attribut: Legt ein Attribut (Eigenschaft) fest, das Sie als Teil des Filters verwenden möchten.

Operator: Legt den logischen Operator fest, der auf den Filter angewandt werden soll. Die gültigen Optionen sind.

Wert: Legt den Attributwert fest, den Sie als Filter verwenden. Sie können das Sternchen (*) als Platzhalter verwenden, um einen Teil eines Werts anzuzeigen. Beispielsweise smi*, *th oder *mit*.

Außerdem können Sie mehrere Attributfilter zu einer Filtergruppe verketten, indem Sie über die Schaltfläche + Rule ein zweites Attribut zur Liste hinzufügen. Falls Sie mehrere Attributfilter verwenden, verknüpfen Sie diese mit dem logischen Operator AND oder OR.

Abbildung 4-2 *Erweiterte Suche konfigurieren*



5 Benutzer verwalten

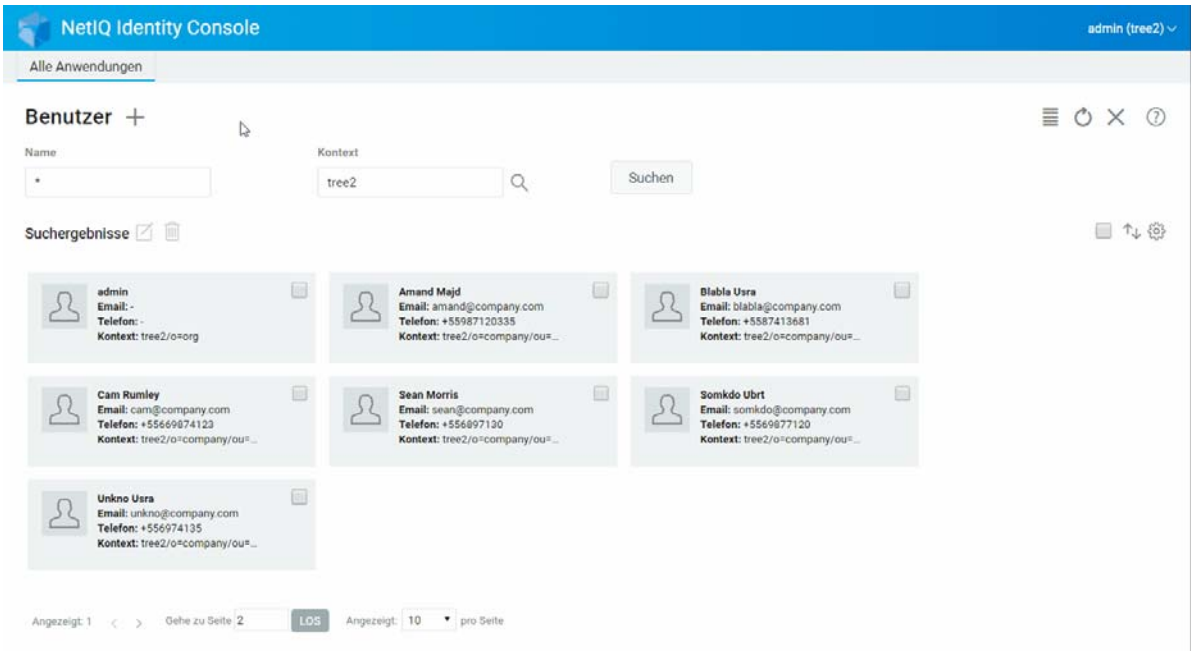
Das Verwalten von Benutzern und deren Netzwerkzugriff ist eine wesentliche Funktion der Datenablage. Mit dem Identity Console-Webportal können Sie die folgenden Aufgaben in Bezug auf Benutzer ausführen:

Erstellen von Benutzern

So erstellen Sie ein neues Benutzerobjekt:

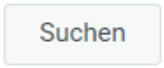
1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Benutzerverwaltung**.
2. Klicken Sie auf das Symbol +.
3. Geben Sie auf der Benutzererstellungsseite mindestens die obligatorischen Benutzerinformationen an. Klicken Sie dann auf die Schaltfläche Erstellen.
   - **Benutzername**
   - **Kontext**
   - **Nachname**
   - **Passwort**
4. Eine Meldung bestätigt das Erstellen des Benutzerobjekts.

Abbildung 5-1 *Benutzer erstellen*



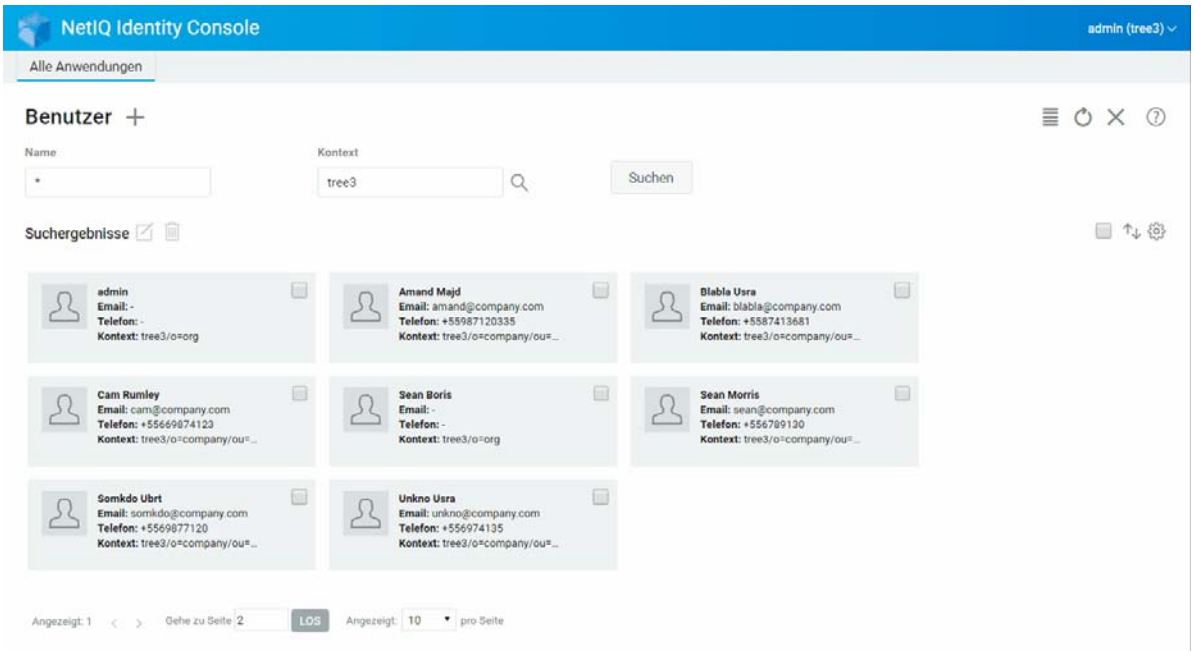
Benutzer löschen

So löschen Sie ein Benutzerobjekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Benutzerverwaltung**.
2. Geben Sie den Namen und den Kontext des Objekts ein oder suchen Sie es mithilfe der Suchfunktion. Klicken Sie dann auf die Schaltfläche 

.
3. Wählen Sie das Benutzerobjekt aus der Benutzerliste aus und klicken Sie auf das Symbol 🗑.
4. Eine Meldung bestätigt das Löschen des Benutzerobjekts.

Abbildung 5-2 *Benutzer löschen*

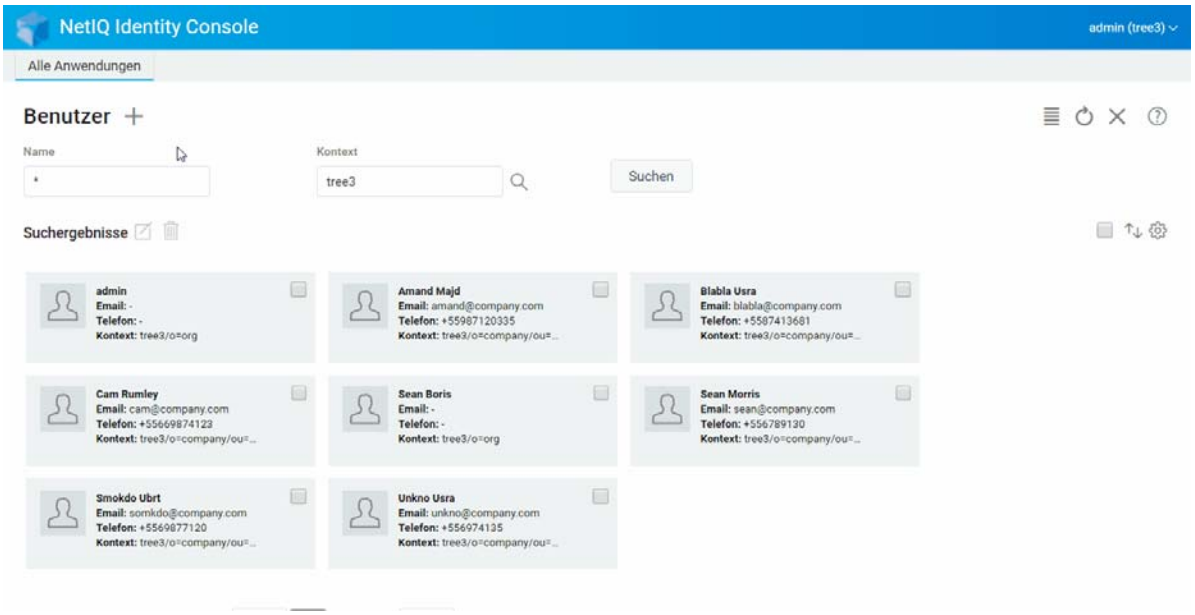


Benutzer ändern

So ändern Sie ein Benutzerobjekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Benutzerverwaltung**.
2. Geben Sie den Namen und den Kontext des Objekts ein oder suchen Sie es mithilfe der Suchfunktion. Klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie das Benutzerobjekt aus der Benutzerliste aus und klicken Sie auf das Symbol .
4. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf die Schaltfläche Speichern.
5. Eine Meldung bestätigt das Ändern des Benutzerobjekts.

Abbildung 5-3 *Benutzer bearbeiten*

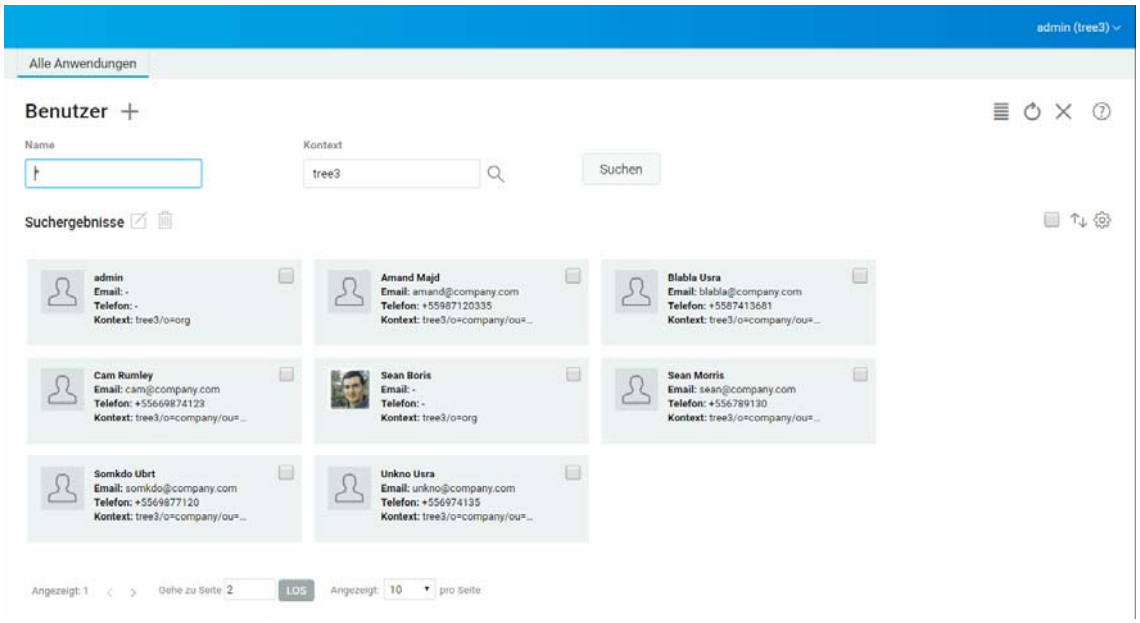


Benutzer suchen

So suchen Sie nach einem Benutzerobjekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Benutzerverwaltung**.
2. Sie können einen Benutzer entweder über den Namen oder über eine Kombination aus Name und Kontext suchen. Geben Sie die erforderlichen Details an und klicken Sie dann auf das Symbol Suchen.

Abbildung 5-4 *Benutzer suchen*

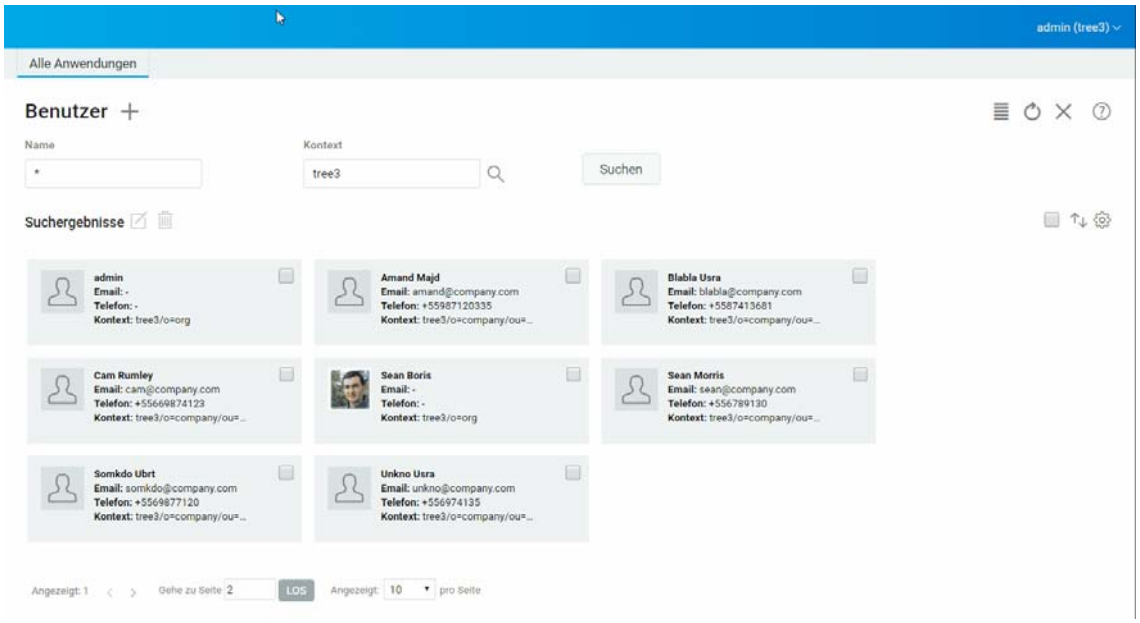


Passwortbeschränkungen festlegen

Über die Funktion der Passwortbeschränkungen können Sie die folgenden Aktionen ausführen:

- Zulassen, dass Benutzer ihr Passwort ändern
- Passwort für die Anmeldung erzwingen
- Passwortstärke festlegen
- Regelmäßige Passwortänderungen erzwingen
- Ablaufdatum für Passwörter festlegen
- Erstellen eindeutiger Passwörter erzwingen
- Kulanzanmeldezeitraum nach Ablauf des Passworts festlegen

Abbildung 5-5 *Passwortbeschränkungen*

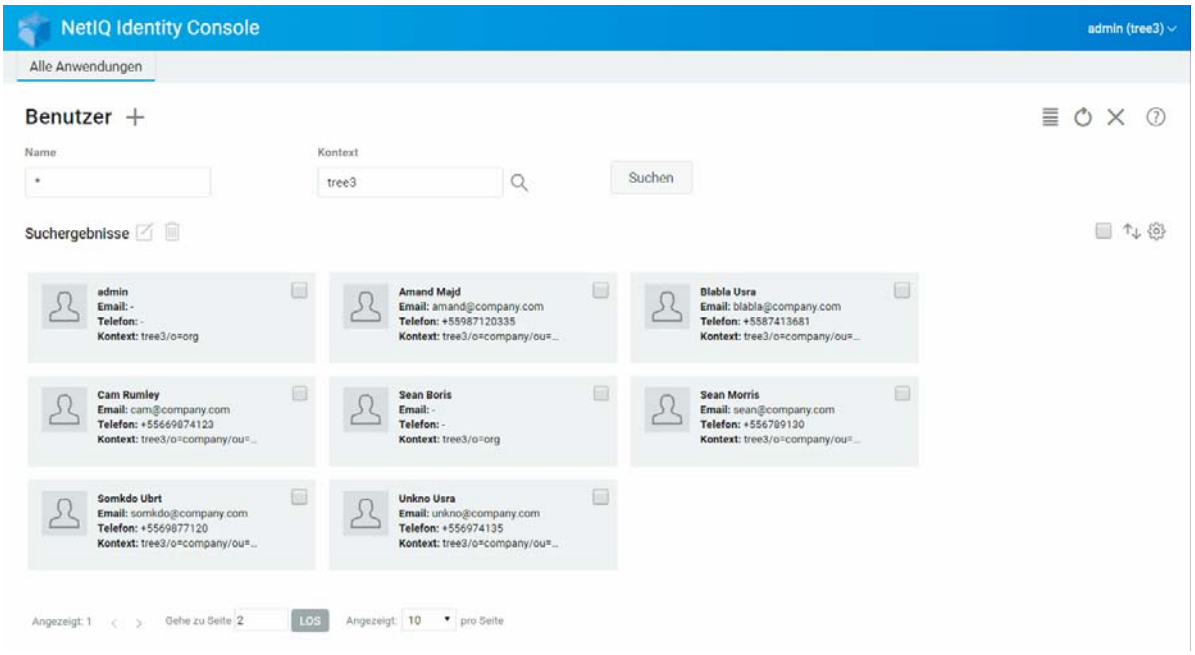


Benutzerkonten deaktivieren und aktivieren

Führen Sie die folgenden Schritte aus, um ein Benutzerkonto zu deaktivieren:

1. Wählen Sie den Benutzer aus, dessen Konto deaktiviert werden soll, und klicken Sie auf das Symbol .
2. Klicken Sie auf die Registerkarte **Beschränkungen** auf der Seite **Benutzer ändern**.
3. Erweitern Sie die Registerkarte **Anmeldebeschränkungen** und aktivieren Sie das Kontrollkästchen **Konto deaktiviert**.
4. Klicken Sie auf das Symbol Speichern.
5. Das Benutzerkonto ist nun deaktiviert. Wenn Sie ein deaktiviertes Benutzerkonto aktivieren möchten, deaktivieren Sie das Kontrollkästchen **Konto deaktiviert**.

Abbildung 5-6 *Benutzerkonten deaktivieren und aktivieren*

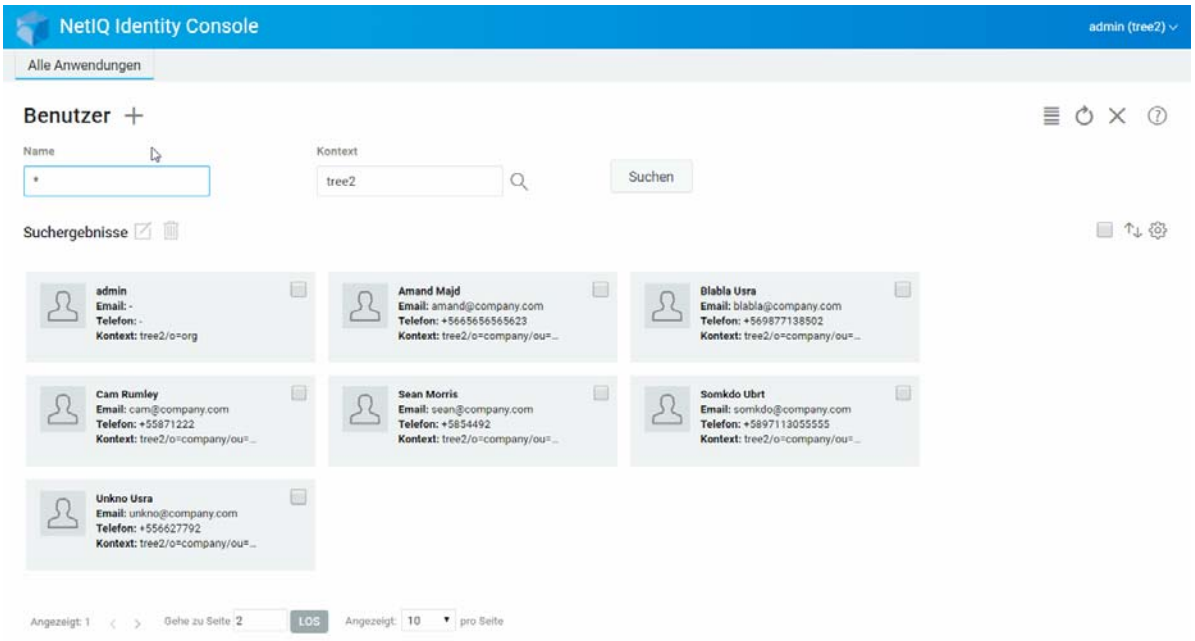


Kontoablaufdatum festlegen

Führen Sie die folgenden Schritte aus, um ein Kontoablaufdatum für Benutzer festzulegen:

1. Wählen Sie den Benutzer aus, für den ein Kontoablaufdatum festgelegt werden soll, und klicken Sie auf das Symbol .
2. Klicken Sie auf die Registerkarte **Beschränkungen** auf der Seite **Benutzer ändern**.
3. Erweitern Sie die Registerkarte **Anmeldebeschränkungen**, aktivieren Sie das Kontrollkästchen **Konto hat Ablaufdatum** und legen Sie ein **Ablaufdatum** fest.
4. Klicken Sie auf das Symbol Speichern.

Abbildung 5-7 *Kontoablaufdatum festlegen*

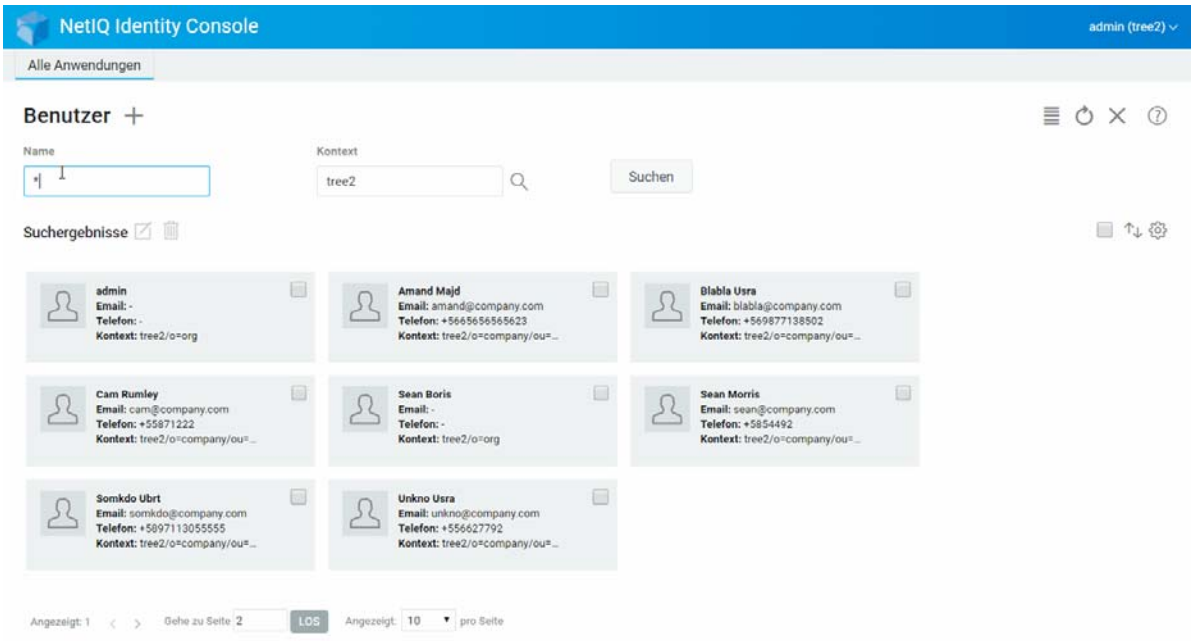


Unbefugtensperre prüfen und löschen

Im Identity Console-Webportal können Sie für jedes Benutzerkonto Details zur Unbefugtensperre anzeigen. So zeigen Sie die Details zur Unbefugtensperre an:

1. Wählen Sie den Benutzer aus, für den Sie Details zur Unbefugtensperre überprüfen möchten, und klicken Sie auf das Symbol .
2. Klicken Sie auf die Registerkarte **Beschränkungen** auf der Seite **Benutzer ändern**.
3. Erweitern Sie die Registerkarte **Unbefugtensperre** und zeigen Sie die Details zur Unbefugtensperre an.
4. Wählen Sie nun die Registerkarte **Sperre aufheben** aus und klicken Sie auf die Schaltfläche Sperre aufheben.
5. Klicken Sie auf die Schaltfläche Speichern.

Abbildung 5-8 *Unbefugtensperre prüfen und löschen*



6 Gruppen verwalten

Gruppen enthalten üblicherweise mehrere Mitglieder. Jeder Benutzer, der eine Gruppe erstellt, wird automatisch Eigentümer dieser Gruppe. Mit der Gruppenverwaltungsfunktion können die folgenden Vorgänge ausgeführt werden:

- „Gruppen erstellen“, auf Seite 35
- „Gruppen löschen“, auf Seite 36
- „Gruppen ändern“, auf Seite 37
- „Gruppenmitglieder hinzufügen oder ändern“, auf Seite 38
- „Gruppen suchen“, auf Seite 39

Weitere Informationen über das Verwenden und Konfigurieren von Gruppenobjekten finden Sie im *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (NetIQ eDirectory 9.2-Administrationshandbuch).

Gruppen erstellen

So erstellen Sie eine Gruppe:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Gruppenverwaltung**.
2. Klicken Sie auf das Symbol +.
3. Geben Sie auf der Gruppenerstellungsseite die folgenden Details ein:
   - Geben Sie den Gruppennamen an.
   - Geben Sie den Kontext an.

   Wählen Sie **Dynamische Gruppe** aus, um die neue Gruppe als dynamische Gruppe der Klasse `dynamicGroup` zu erstellen. Andernfalls wird die Gruppe als statische Gruppe erstellt.

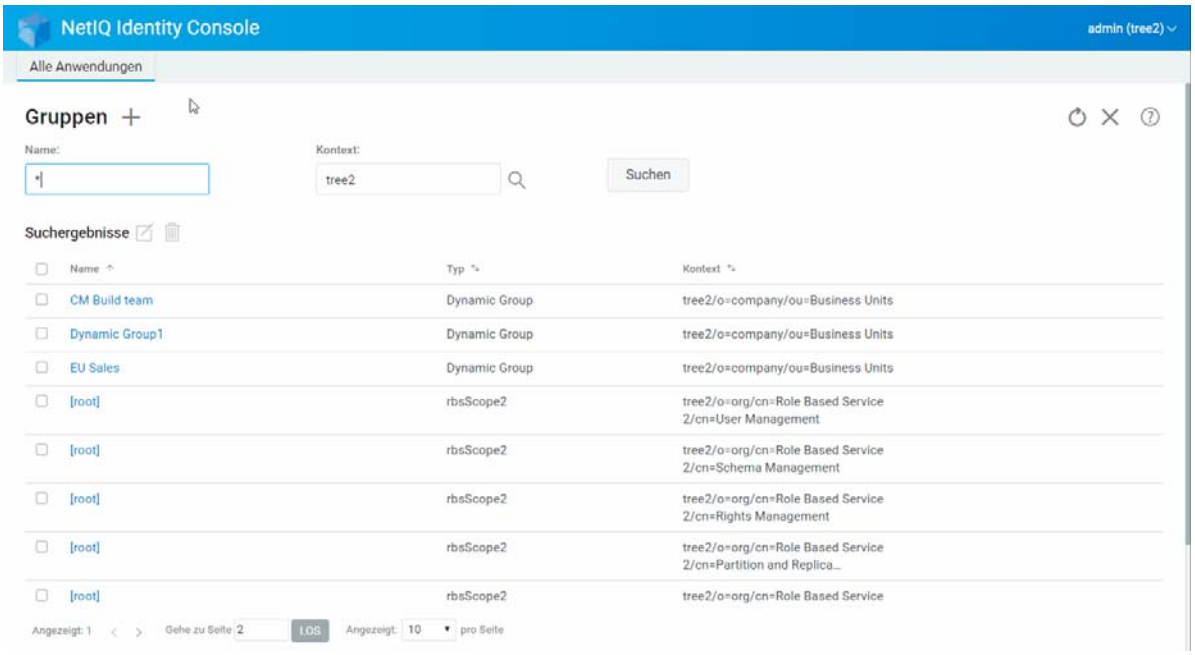
   Wählen Sie **Verschachtelte Gruppe** aus, um die neue Gruppe als verschachtelte Gruppe mit der Zusatzklasse `nestedGroupAux` zu erstellen.

   HINWEIS: Befolgen Sie das unter Objekte ändern beschriebene Verfahren, wenn Sie eine statische Gruppe in eine dynamische oder in eine verschachtelte Gruppe umwandeln möchten. Dadurch wird das ausgewählte Gruppenobjekt so erweitert, dass es zur Klasse `dynamicGroupAux` bzw. `nestedGroupAux` gehört.

   Eine Gruppe kann entweder verschachtelt oder dynamisch sein. Eine Gruppe kann nicht beides sein.

   ---
4. Nachdem Sie die erforderlichen Details festgelegt haben, klicken Sie auf die Schaltfläche Erstellen.
5. Eine Meldung bestätigt das Erstellen der Gruppe.

Abbildung 6-1 *Gruppen erstellen*

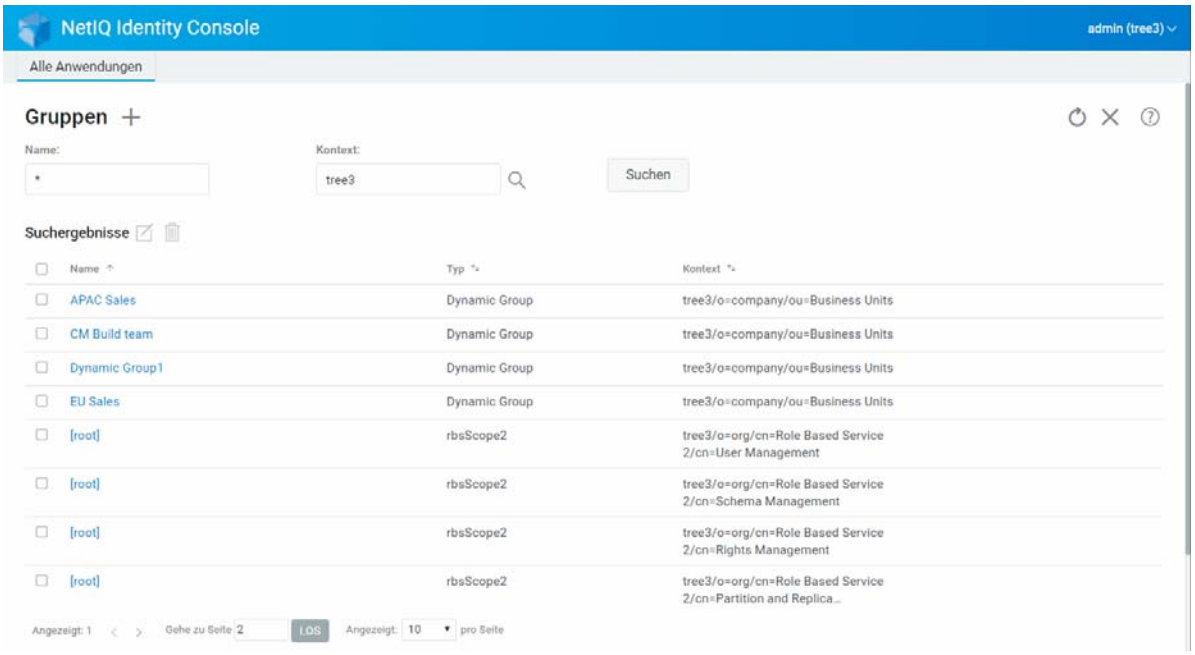


Gruppen löschen

So löschen Sie eine Gruppe:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Gruppenverwaltung**.
2. Geben Sie den Namen und den Kontext der Gruppe an oder suchen Sie die Gruppe mithilfe der Suchfunktion. Klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie die zu löschende Gruppe aus und klicken Sie auf das Symbol 🗑.
4. Eine Meldung bestätigt das Löschen der Gruppe.

Abbildung 6-2 *Gruppen löschen*

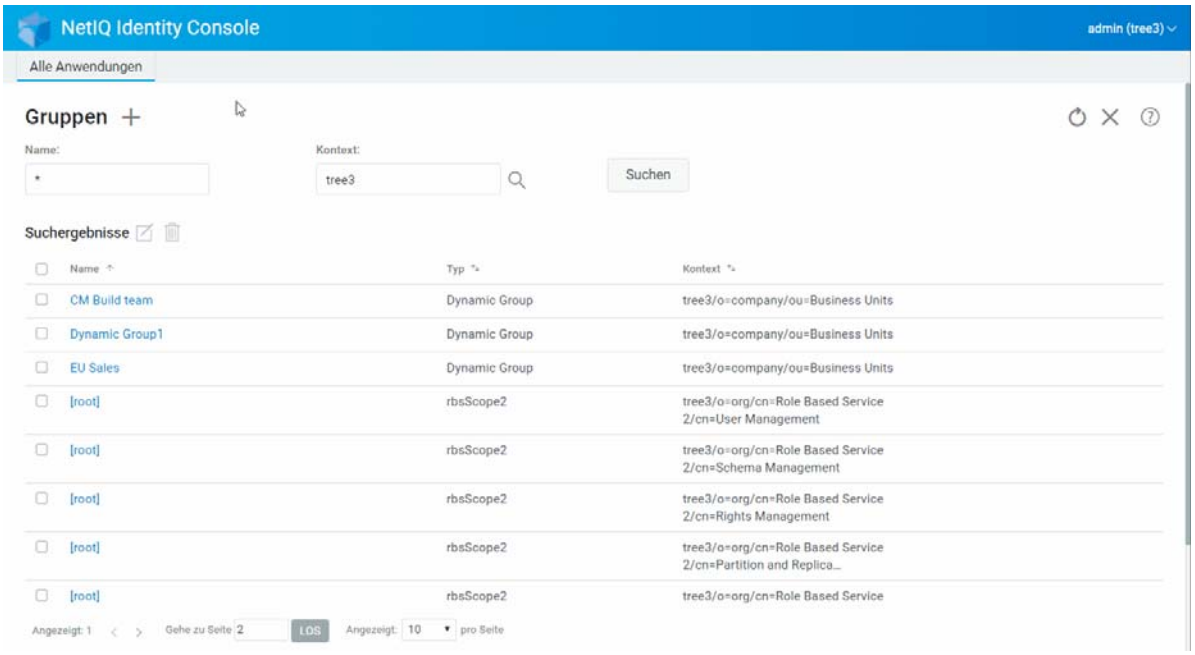


Gruppen ändern

So ändern Sie eine Gruppe:

1. Klicken Sie auf der Identity Console-Landeseite auf **Gruppenverwaltung**.
2. Geben Sie den Namen und den Kontext der Gruppe ein und klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie die zu ändernde Gruppe aus und klicken Sie auf das Symbol .
4. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf die Schaltfläche Speichern.
5. Eine Meldung bestätigt das Ändern der Gruppe.

Abbildung 6-3 *Gruppen ändern*

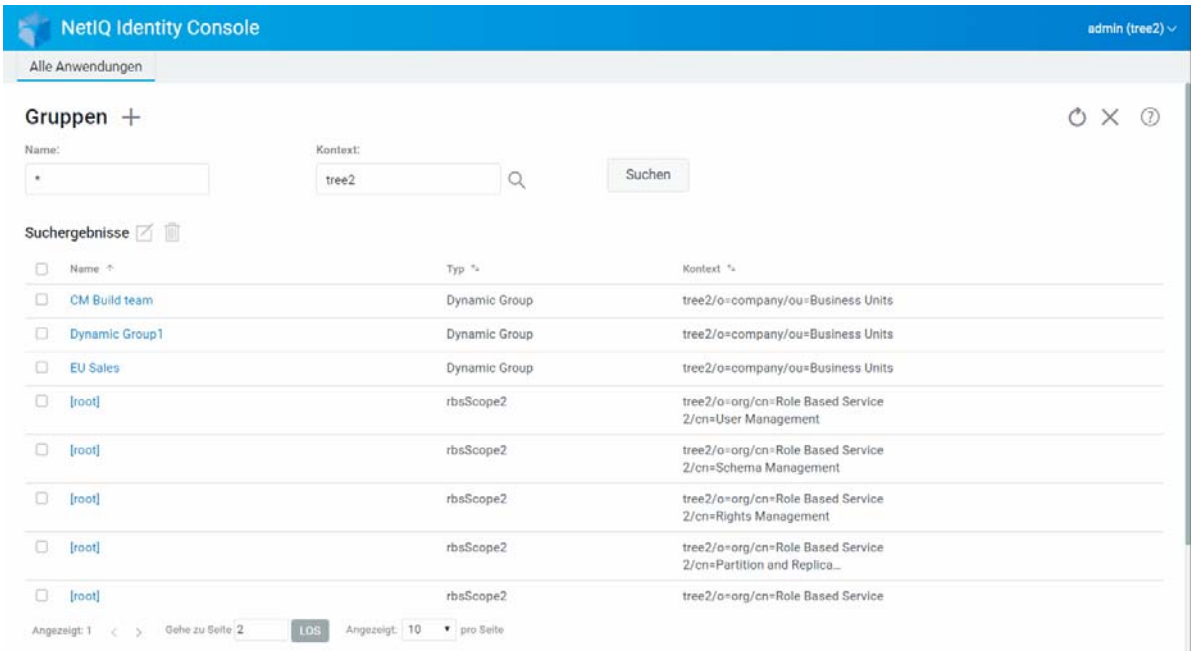


Gruppenmitglieder hinzufügen oder ändern

So können Sie Gruppenmitglieder hinzufügen oder ändern:

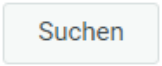
1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Gruppenverwaltung**.
2. Geben Sie den Namen und den Kontext der Gruppe ein und klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie die Gruppe aus und klicken Sie auf das Symbol .
4. Klicken Sie auf die Registerkarte **Mitglieder** auf der Seite **Gruppe ändern**.
5. Fügen Sie über das Symbol ein neues Mitglied zur Gruppe hinzu. Klicken Sie auf das Symbol , wenn Sie Mitglieder aus der Gruppe entfernen möchten.
6. Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf das Symbol Speichern.
7. Eine Meldung bestätigt das Ändern der Gruppe.

Abbildung 6-4 *Gruppenmitglieder hinzufügen oder ändern*



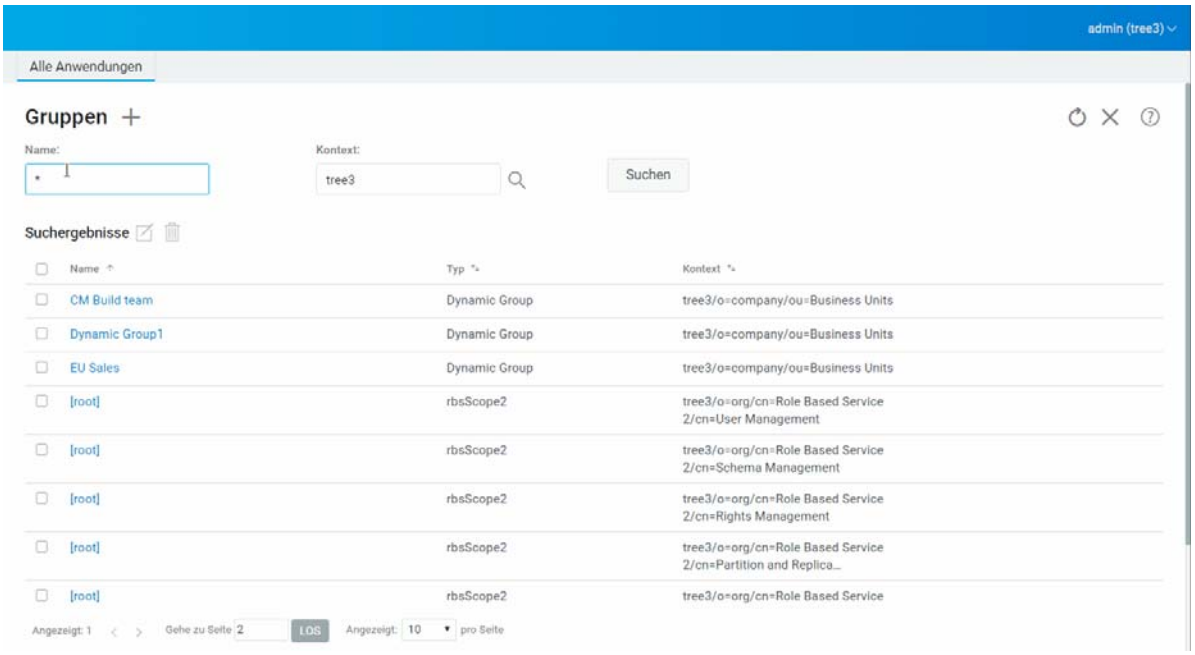
Gruppen suchen

So suchen Sie nach Gruppen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Gruppenverwaltung**.
2. Sie können Gruppen entweder über den Namen oder über eine Kombination aus Name und Kontext suchen.
3. Geben Sie die erforderlichen Details an und klicken Sie dann auf das Symbol 

.

Abbildung 6-5 *Gruppen suchen*



7 Objekte verwalten

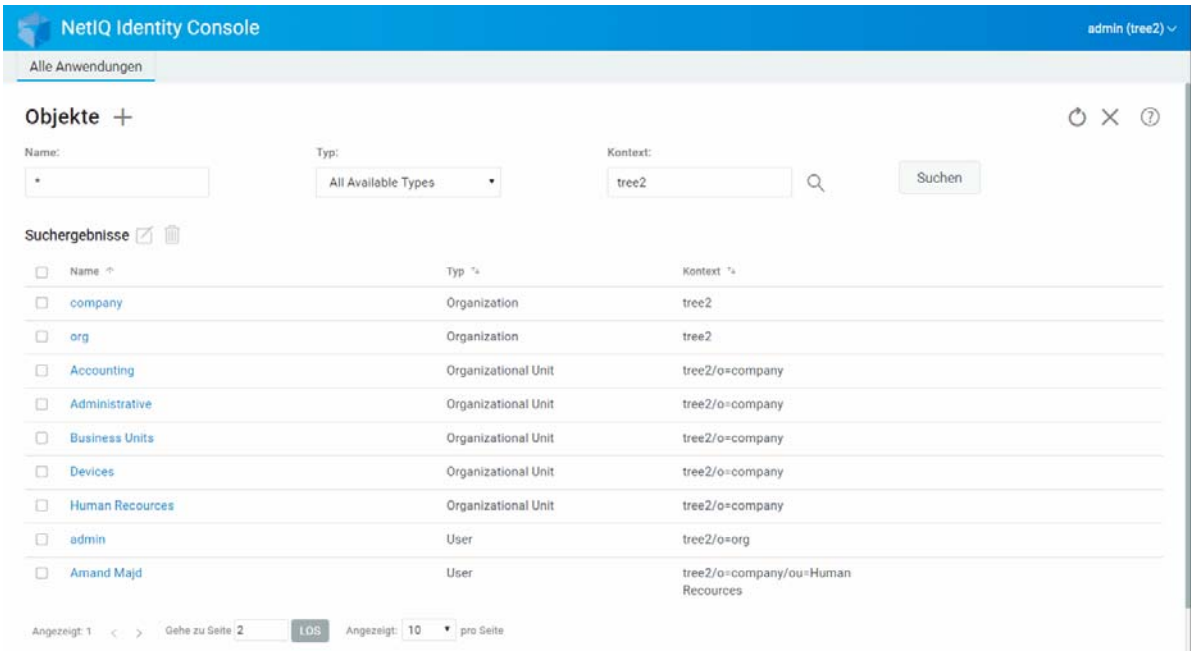
Mit Identity Console können Sie verschiedene Objekte in der Datenablage verwalten. Das Modul bietet Funktionen zum Erstellen, Ändern, Löschen und Suchen von Objekten.

Objekte erstellen

So erstellen Sie ein neues Objekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Objektverwaltung**.
2. Klicken Sie auf das Symbol  .
3. Geben Sie auf der Objekterstellungsseite die folgenden Details ein:
   - Geben Sie einen Objektnamen an.
   - Geben Sie den Typ an.
   - Geben Sie den Kontext an.
4. Nachdem Sie alle erforderlichen Details eingegeben haben, klicken Sie auf **Weiter** > **Erstellen**.
5. Eine Meldung bestätigt das Erstellen des Objekts.

Abbildung 7-1 *Objekte erstellen*

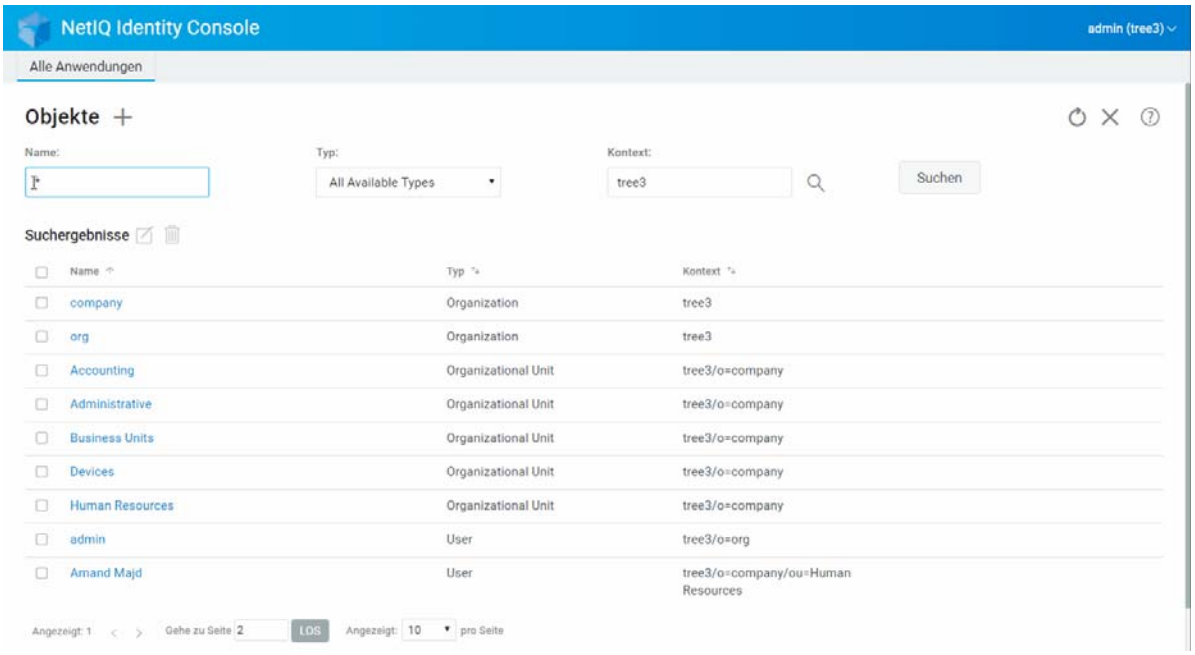


Objekte löschen

So löschen Sie Objekte:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Objektverwaltung**.
2. Geben Sie den Namen, den Typ und den Kontext des Objekts an oder suchen Sie es mithilfe der Suchfunktion. Klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie das Objekt aus der Suchliste aus und klicken Sie auf das Symbol 🗑.
4. Eine Meldung bestätigt das Löschen des Objekts.

Abbildung 7-2 *Objekte löschen*

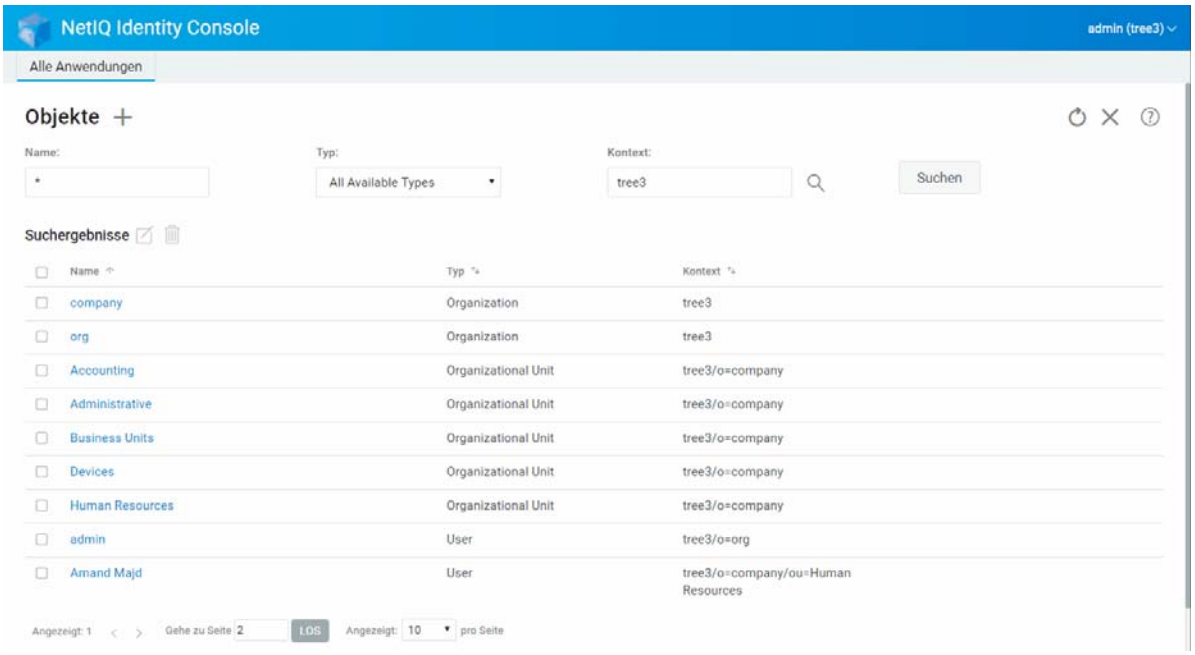


Objekte ändern

So ändern Sie ein Objekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Objektverwaltung**.
2. Geben Sie den Namen, den Typ und den Kontext des Objekts an und klicken Sie auf die Schaltfläche Suchen.
3. Wählen Sie das Objekt aus der Suchliste aus und klicken Sie auf das Symbol .
4. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf die Schaltfläche Speichern.
5. Eine Meldung bestätigt das Ändern des Objekts.

Abbildung 7-3 *Objekte ändern*

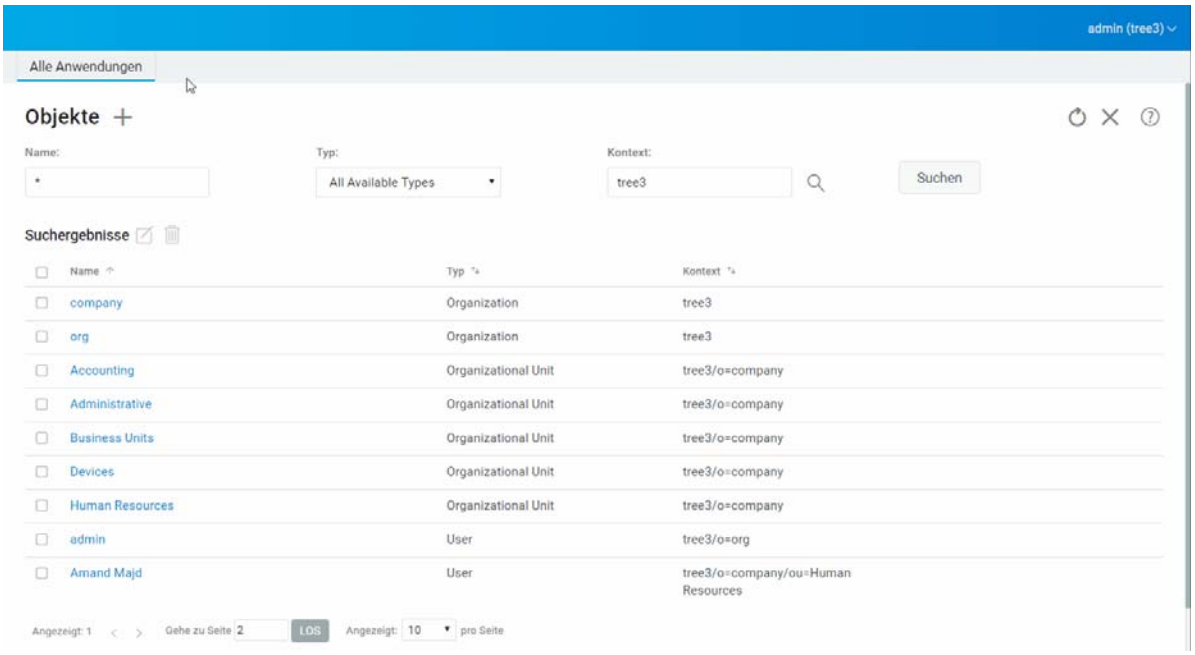


Objekte suchen

So suchen Sie nach einem Objekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Objektverwaltung**.
2. Sie können Objekte entweder über den Namen oder über eine Kombination aus Name, Typ und Kontext suchen.
3. Nachdem Sie die erforderlichen Details festgelegt haben, klicken Sie auf die Schaltfläche Suchen.

Abbildung 7-4 *Objekte suchen*



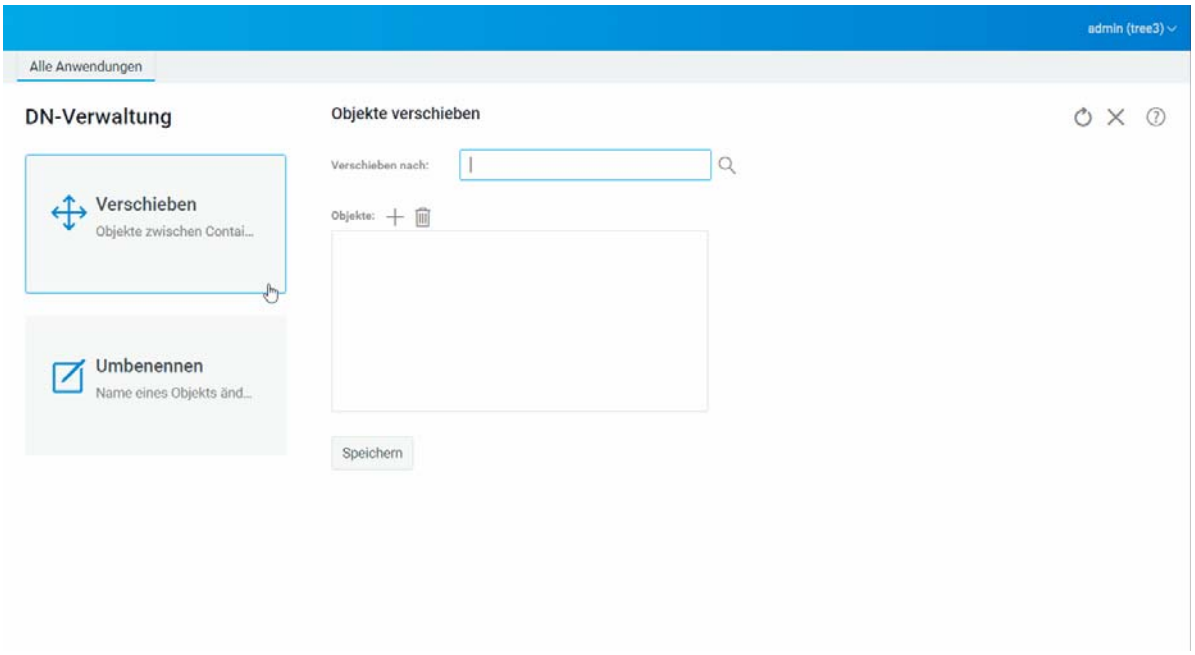
Objekte verschieben

So verschieben Sie ein Objekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **DN-Verwaltung**.
2. Die Option **Objekt verschieben** ist standardmäßig ausgewählt.
3. Wählen Sie im Feld **Verschieben nach** den Container aus, in den Sie das Objekt verschieben möchten.
4. Klicken Sie auf das Symbol +, um das zu verschiebende Objekt zu einem anderen Container hinzuzufügen.

   Um ein ausgewähltes Objekt zu entfernen, klicken Sie auf das Symbol 🗑.
5. Klicken Sie auf die Schaltfläche Speichern.
6. Eine Meldung bestätigt das erfolgreiche Verschieben des Objekts.

Abbildung 7-5 *Objekte verschieben*

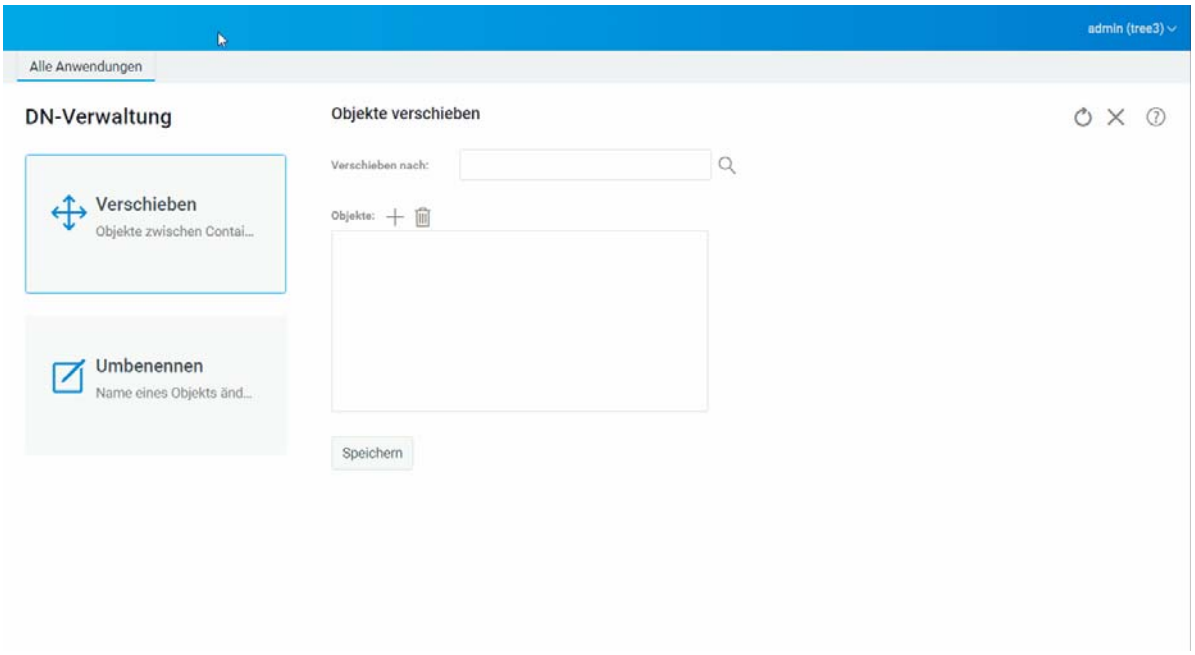


Objekte umbenennen

So benennen Sie ein Objekt um:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **DN-Verwaltung**.
2. Wählen Sie die Option **Objekt umbenennen** aus.
3. Suchen Sie mithilfe der Suchfunktion im Feld **Objektname** das Objekt, das umbenannt werden soll.
4. Geben Sie im Feld **Neuer Name** nur den neuen Namen des Objekts an, nicht den Kontext.
5. Wählen Sie, falls gewünscht, die Option zum Speichern des alten Namens.
6. Klicken Sie auf die Schaltfläche Speichern.
7. Eine Meldung bestätigt das erfolgreiche Umbenennen des Objekts.

Abbildung 7-6 *Objekte umbenennen*



8 Rechte verwalten

Rechte beziehen sich hier auf eDirectory-Trustee-Rechte und -Trustees. Wenn Sie einen Baum erstellen, bieten die standardmäßigen Rechtezuweisungen allgemeine Zugriffs- und Sicherheitsfunktionen für Ihr Netzwerk. Mit Identity Console können Sie die folgenden Aufgaben in Bezug auf Rechte ausführen:

- „Filter für vererbte Rechte ändern“, auf Seite 49
- „Trustee-Rechte ändern“, auf Seite 50
- „Effektive Rechte anzeigen“, auf Seite 51

Weitere Informationen zu eDirectory-Rechten finden Sie im *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (NetIQ eDirectory 9.2-Administrationshandbuch).

Filter für vererbte Rechte ändern

eDirectory bietet einen Filter für vererbte Rechte, mit dem das Vererben von Rechten an einzelne untergeordnete Elemente gesperrt werden kann.

Weitere Informationen zu Filtern für vererbte Rechte finden Sie im *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (NetIQ eDirectory 9.2-Administrationshandbuch).

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Rechteverwaltung**.
2. Wählen Sie **Filter für vererbte Rechte** aus.

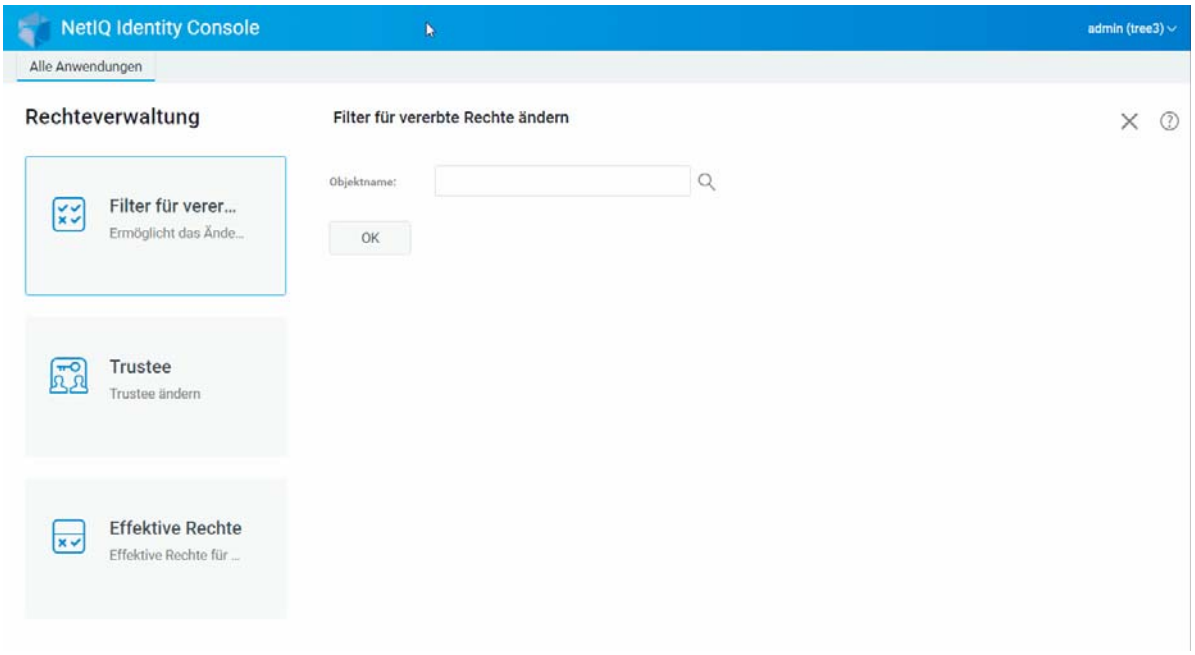
   HINWEIS: Standardmäßig ist der Filter für vererbte Rechte aktiviert.

3. Geben Sie den vollständigen Namen des Objekts an, dessen Filter für vererbte Rechte Sie ändern möchten, oder suchen Sie es über das Objektauswahlsymbol  . Klicken Sie dann auf **OK**.

   Daraufhin wird eine Liste der Filter für vererbte Rechte angezeigt, die bereits für das Objekt definiert wurden.
4. Bearbeiten Sie unter **Eigenschaften** die Liste der Filter für vererbte Rechte je nach Bedarf und klicken Sie dann auf **Anwenden**.

   Zur Bearbeitung der Filterliste benötigen Sie das Supervisor- oder Zugriffssteuerungsrecht für die ACL-Eigenschaft des Objekts. Sie können Filter festlegen, die vererbte Rechte für das gesamte Objekt, für alle Eigenschaften des Objekts oder für einzelne Eigenschaften blockieren.

Abbildung 8-1 *Filter für vererbte Rechte ändern*



Trustee-Rechte ändern

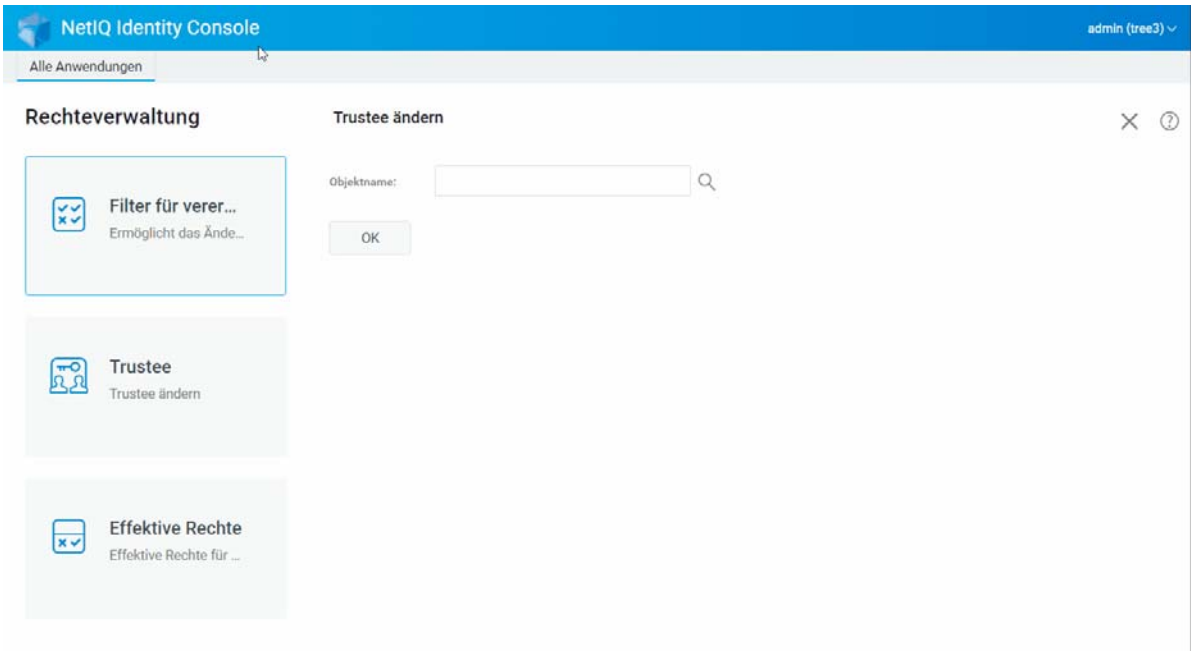
Ein Trustee ist ein Objekt, das ausdrückliche Rechte für ein anderes Objekt in Ihrem Verzeichnisbaum erhalten hat. So bearbeiten Sie die Trustee-Liste für ein bestimmtes Objekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Rechteverwaltung**.
2. Wählen Sie **Trustee** aus.
3. Geben Sie das Objekt an, dessen Trustee-Liste Sie anzeigen möchten, oder suchen Sie es mit dem Objektauswahlsymbol . Klicken Sie dann auf **OK**.

   Dadurch wird eine Liste der dem Objekt zurzeit zugewiesenen Trustees geöffnet.
4. Bearbeiten Sie die Trustee-Liste wie gewünscht und klicken Sie auf **OK**.

   - Um einen Trustee hinzuzufügen, klicken Sie auf das Symbol .
   - Um einen Trustee zu entfernen, aktivieren Sie das Kontrollkästchen des Trustees und klicken Sie auf das Symbol .
   - Bearbeiten Sie die Rechtezuweisung eines Trustee, indem Sie auf den Link **Zugewiesene Rechte** für diesen Trustee klicken.

Abbildung 8-2 *Trustee-Rechte ändern*



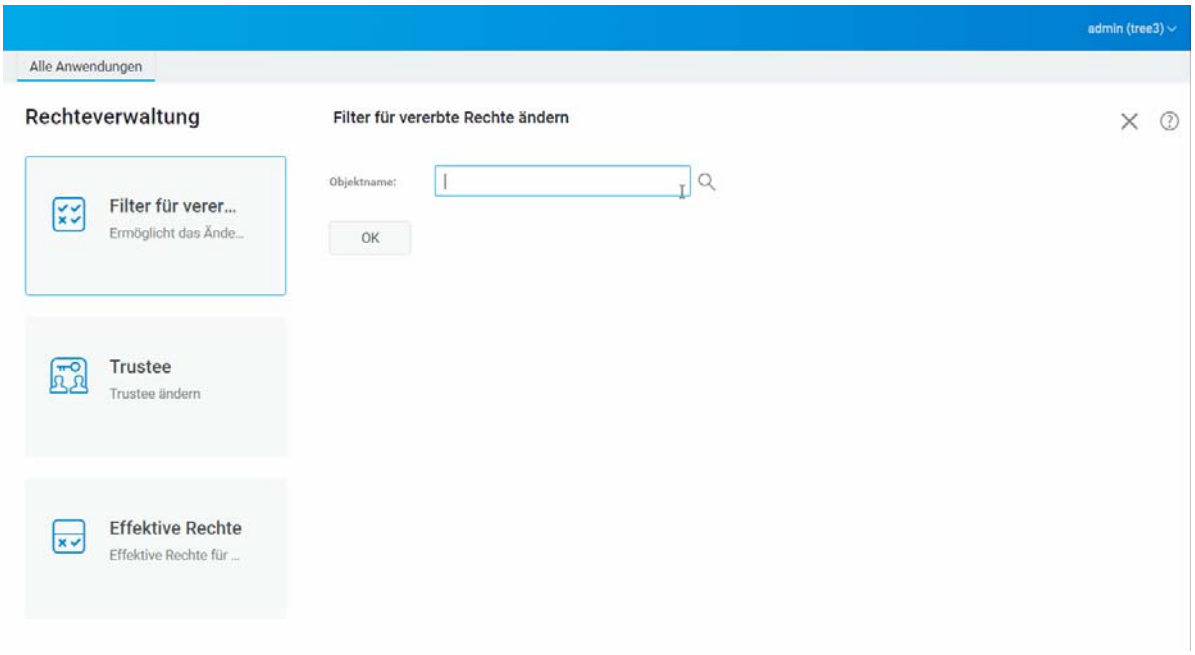
Effektive Rechte anzeigen

Die effektiven Rechte sind die Kombination aus ausdrücklichen und vererbten Rechten, die ein Objekt an einem bestimmten Punkt im Verzeichnisbaum aufweist. So zeigen Sie die effektiven Rechte eines Objekts für ein anderes Objekt an:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Rechteverwaltung**.
2. Wählen Sie **Effektive Rechte** aus.
3. Geben Sie den Namen des Trustees an, dessen Rechte Sie anzeigen möchten, oder suchen Sie ihn über das Objektauswahlsymbol . Klicken Sie dann auf **OK**.
4. Geben Sie im Feld für den Objektnamen den Namen des Objekts an, für das Sie die effektiven Rechte des Trustees anzeigen möchten.

   eDirectory ermittelt die effektiven Rechte und zeigt sie im Feld **Effektive Rechte** an.

Abbildung 8-3 *Effektive Rechte anzeigen*



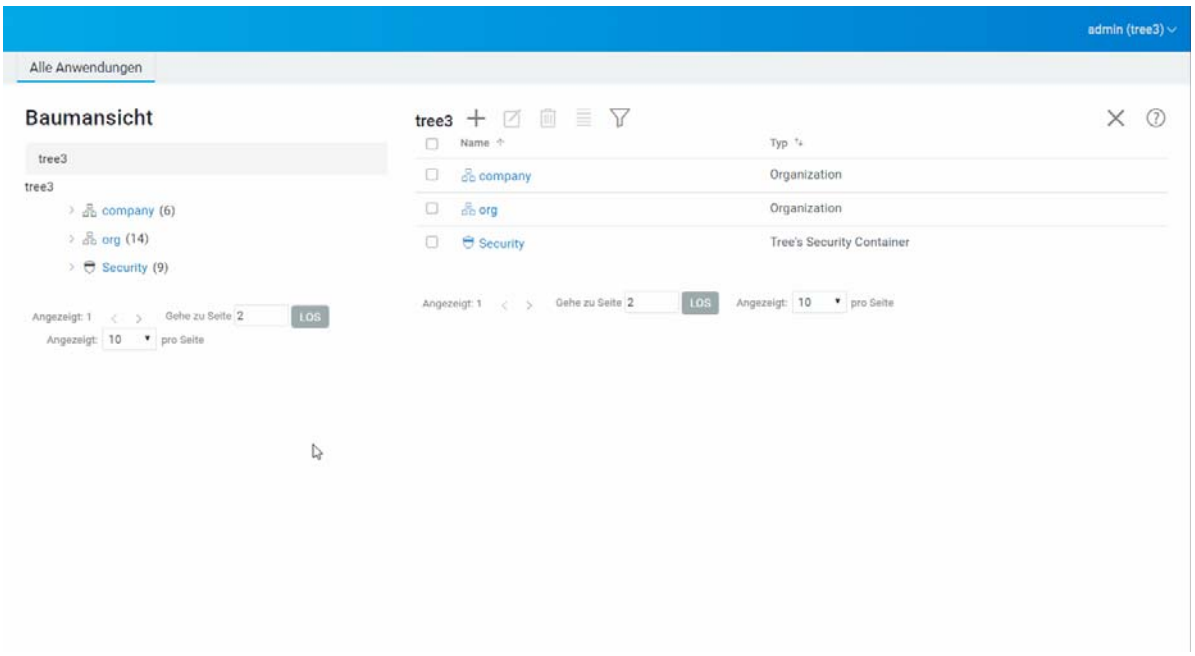
9 Baumansicht

In der Baumansicht können Sie einen Verzeichnisbaum durchsuchen und Objekte im Baum erstellen, löschen oder ändern. Die Baumansicht enthält einen Navigationsrahmen und einen Inhaltsrahmen.

Navigationsrahmen der Baumansicht

Der Navigationsrahmen in der Baumansicht zeigt die Verzeichnisstruktur. Der Navigationsrahmen zeigt Container einschließlich Volume (Dateisystem), Objekten usw. an. Alle unter dem Navigationsrahmen angezeigten Optionen sind anklickbar, um Ihnen das Durchsuchen der Verzeichnisstruktur zu erleichtern. Standardmäßig enthält der Navigationsrahmen bis zu 10 untergeordnete Objekte pro Container. Sie können diese Einstellung jedoch unterhalb des Navigationsrahmenbereichs in der Baumansicht ändern.

Abbildung 9-1 *Navigationsrahmen in der Baumansicht*



Baumansicht Inhaltsrahmen

Wenn Sie eines der Containerobjekte im Navigationsrahmen auswählen, werden im Inhaltsrahmen alle Objekte in diesem Container angezeigt. Im Inhaltsrahmen können die Verzeichnisobjekte angezeigt und geändert werden. Der Inhaltsrahmen verfügt über einen Kopfbereich, in dem verschiedene Aktionen zur Verfügung stehen:

Titelleiste: Die Titelleiste des Inhaltsrahmens zeigt den Namen des zurzeit ausgewählten Containerobjekts an.

Objektlisten-Kopftext: Der Objektlisten-Kopftext bietet Zugriff auf die folgenden Elemente:

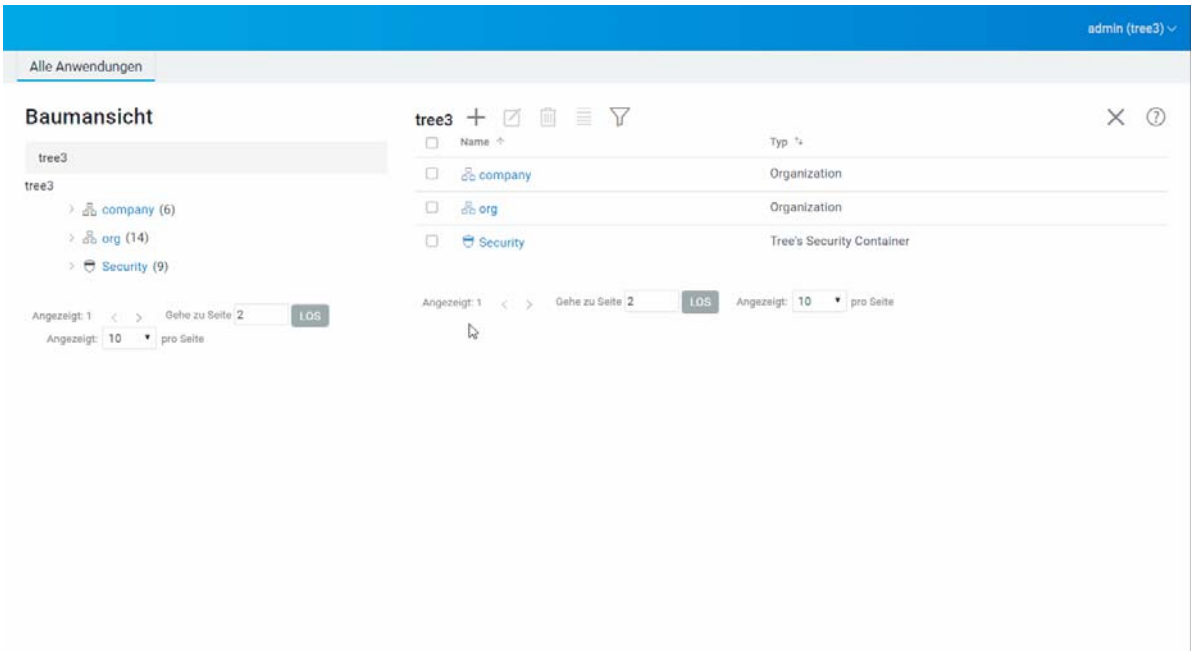
- **Hinzufügen**: Klicken Sie auf das Symbol  , um ein neues Objekt hinzuzufügen.
- **Ändern**: Wählen Sie ein Objekt aus und klicken Sie auf das Symbol  , um es zu ändern. Dies öffnet das Eigenschaftsbuch des ausgewählten Objekts, wo Sie die Attribute ändern können. Es ist nicht möglich, mehrere Objekte gleichzeitig zu ändern.
- **Löschen**: Wählen Sie Objekte aus und klicken Sie auf das Symbol  , um die ausgewählten Objekte zu löschen. Es besteht die Möglichkeit, mehrere Objekte gleichzeitig zu löschen. Nicht-Blatt-Objekte können nicht gelöscht werden.
- **Aktionen**: Wählen Sie Objekte aus und klicken Sie auf das Symbol  . Ein Dropdown-Menü mit den unterstützten Aufgaben für die ausgewählten Objekte wird angezeigt. Um eine Aufgabe auszuführen, wählen Sie sie aus dem Dropdown-Menü aus und geben Sie die erforderlichen Informationen ein.
- **Objektanzahl**: In der Baumansicht wird die Anzahl der Objekte auf der aktuellen Seite am unteren Seitenrand angezeigt. Standardmäßig werden im Inhaltsrahmen bis zu 20 untergeordnete Objekte pro Container angezeigt. Sie können diese Einstellung jedoch ändern.
- **Alle auswählen:** Über das Kontrollkästchen im Kopfbereich können alle Objekte auf der aktuellen Seite auf einmal ausgewählt werden.
- **Sortieren**: Die Einträge können nach den Spalten **Name** und **Typ** sortiert werden. Klicken Sie auf einen beliebigen dieser Spaltenköpfe, um zwischen aufsteigender und absteigender Reihenfolge der alphabetischen Objektsortierung umzuschalten.
- **Suchfilter**: Klicken Sie auf das Symbol  , um das Popup-Fenster für die Filterfunktion zu öffnen. Mit dieser Option können Sie einen Filter erstellen, der die Anzahl der in der Objektliste angezeigten Objekte begrenzt. Sie können je nach Bedarf nach Objekttyp oder nach Objektname filtern.

  Wählen Sie die Option  aus, um den Dialog für den erweiterten Filter zu öffnen. Hier können Sie einen Filter mit nahezu beliebigen Objektattributen erstellen. Weitere Informationen finden Sie unter „Erweiterte Suche konfigurieren“, auf Seite 24.

Um eine Aktion für ein Objekt auszuführen, aktivieren Sie das Kontrollkästchen des Objekts und wählen Sie dann das Aktionssymbol  im Kopfbereich der Objektliste aus. Wählen Sie das Objekt der aktuellen Ebene aus, um eine Aktion für den Container auszuführen, den Sie gerade durchsuchen. Mit dieser Option können die folgenden Aktionen ausgeführt werden:

- „Filter für vererbte Rechte ändern“, auf Seite 49
- „Trustee-Rechte ändern“, auf Seite 50
- „Objekte erweitern“, auf Seite 63
- „Objekte umbenennen“, auf Seite 46
- Passwort festlegen
- „Effektive Rechte anzeigen“, auf Seite 51

Abbildung 9-2 *Inhaltsrahmen in der Baumansicht*



10 Schema verwalten

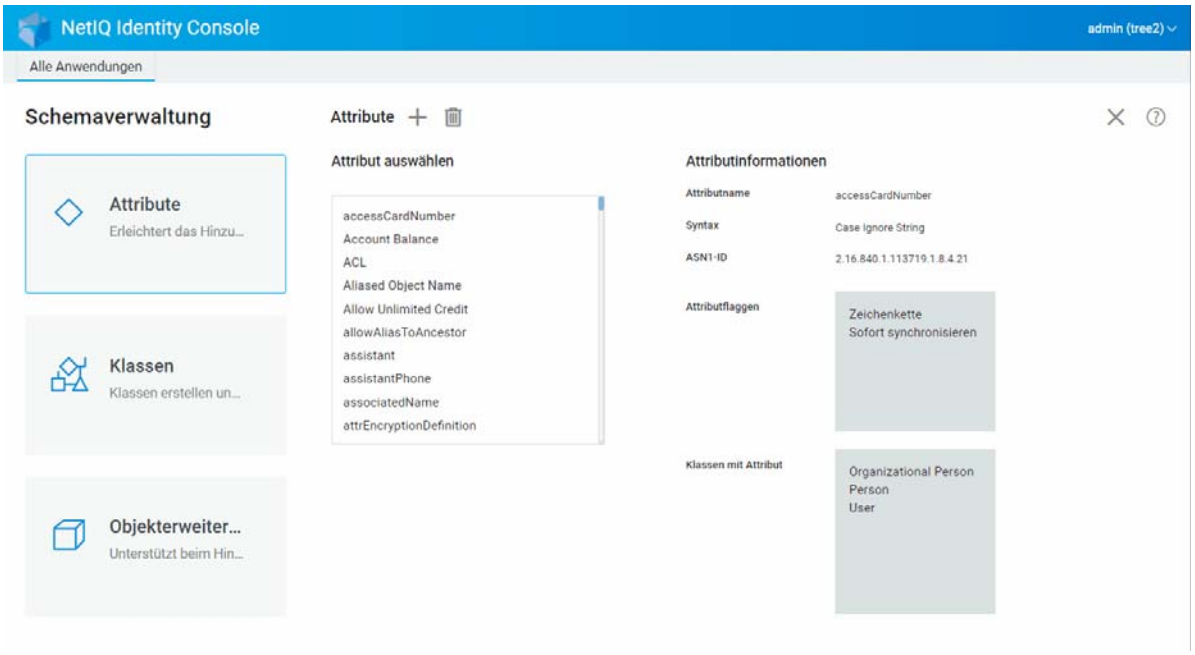
Das Verzeichnisschema definiert, welche Objekttypen (wie Benutzer, Drucker oder Gruppen) im Baum erstellt werden können und welche Informationen für die Objekterstellung erforderlich bzw. optional sind. Mit Identity Console können Sie die folgenden Aufgaben in Bezug auf Schemas ausführen:

Attribute erstellen

Sie können eigene Attributtypen definieren und diese einer vorhandenen Objektklasse als optionale Attribute hinzufügen. Sie können einer vorhandenen Klasse jedoch keine obligatorischen Attribute hinzufügen. So erstellen Sie ein Attribut:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Schemaverwaltung**.
2. Klicken Sie auf das Symbol +.
3. Geben Sie auf der Attributerstellungsseite die folgenden Details ein:
   - Attributname
   - ASN1-ID (optional)
   - Syntax
   - Attributflaggen
4. Nachdem Sie alle erforderlichen Details eingegeben haben, klicken Sie auf die Schaltfläche Erstellen.
5. Eine Meldung bestätigt das Erstellen des Attributs.

Abbildung 10-1 *Attribute erstellen*



Klassen erstellen

Über die Option **Schemaverwaltung** können Sie eigene Klassen definieren. Anschließend können Sie einzelne Objekte mit den in diesen Klassen definierten Eigenschaften erweitern. So erstellen Sie eine Klasse:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Schemaverwaltung** und wählen Sie **Klassen** aus.
2. Klicken Sie auf das Symbol +.
3. Geben Sie auf der Attributerstellungsseite die folgenden Details ein:
   - Klassenname
   - ASN1-ID (optional)
   - Klassenflaggen: Wählen Sie eine der folgenden Klassenflaggen aus:
     - **Effektive Klasse:** Setzen Sie diese Flagge, wenn Sie eine effektive Klasse erstellen möchten, die zum Erstellen von Objekten verwendet werden kann.
     - **Nicht effektive Klasse:** Wird als Platzhalter für eine Gruppe von Attributen verwendet. Eine nicht effektive Klasse kann nicht zum Erstellen von Objekten verwendet werden. Jedoch kann sie als eine Klasse angegeben werden, aus der andere Klassen Attribute erben können. Die Klasse "Person" ist beispielsweise eine nicht effektive Klasse mit Attributen, die an die Klasse "Benutzer" vererbt wurden.
     - **Zusatzklasse:** Eine Sammlung von Attributen, die nur einzelnen Objekten, jedoch nicht ganzen Klassen zugeordnet werden können.

- **Containerklasse:** Setzen Sie diese Flagge, wenn Sie diese Klasse zu einer Containerklasse machen möchten. Wenn diese Klasse zum Erstellen von Objekten verwendet wird, werden diese Objekte zu Containerobjekten (z. B. organisatorische Einheiten). Setzen Sie diese Flagge nicht für ein Blattobjekt.

HINWEIS: Wenn Sie effektive und nicht effektive Klassen auswählen, müssen Sie außerdem Werte für die übergeordnete Klasse festlegen. Wenn Sie eine Zusatzklasse auswählen, ist die übergeordnete Klasse optional.

---

4. Nachdem Sie die erforderlichen Details eingegeben haben, klicken Sie auf **Weiter**.
5. Wählen Sie im nächsten Bildschirm die optionalen Attribute, obligatorischen Attribute und Benennungsattribute aus und klicken Sie auf **OK**.
6. Eine Meldung bestätigt das Erstellen der Klasse.

Einer Klasse Attribute zuweisen

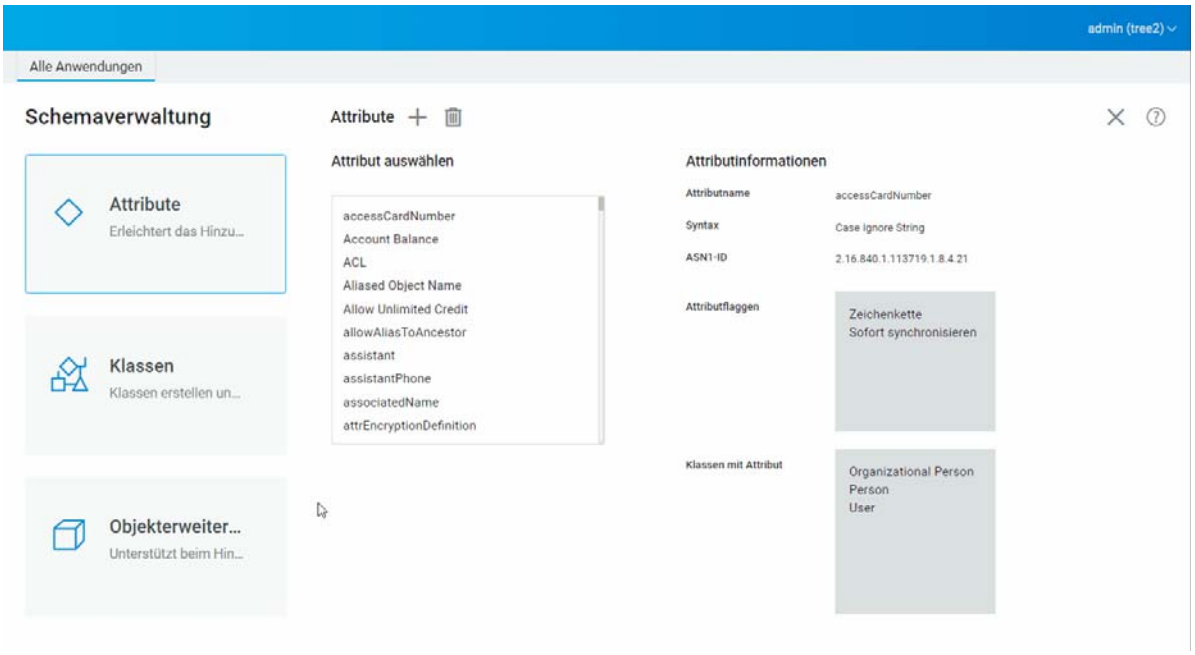
Sie können vorhandenen Klassen optionale Attribute hinzufügen, wenn sich der Informationsbedarf Ihrer Organisation ändert oder wenn Sie die Zusammenführung von Bäumen beabsichtigen. So fügen Sie ein Attribut zu einer vorhandenen Klasse hinzu:

HINWEIS: Obligatorische Attribute können nur während der Klassenerstellung festgelegt werden. Ein obligatorisches Attribut ist ein Attribut, das bei der Erstellung eines Objekts die Eingabe eines Werts erfordert.

---

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Schemaverwaltung** und wählen Sie **Klassen** aus.
2. Klicken Sie auf eine der unter **Klasse auswählen** aufgeführten Klassen.
3. Rechts im Bildschirm werden die entsprechenden Klasseninformationen angezeigt.
4. Klicken Sie auf die Schaltfläche + neben der Option **Attribute** und wählen Sie die Attribute aus, die Sie hinzufügen möchten. Klicken Sie dann auf **Hinzufügen** > **Speichern**.

Abbildung 10-2 *Einer Klasse Attribute zuweisen*

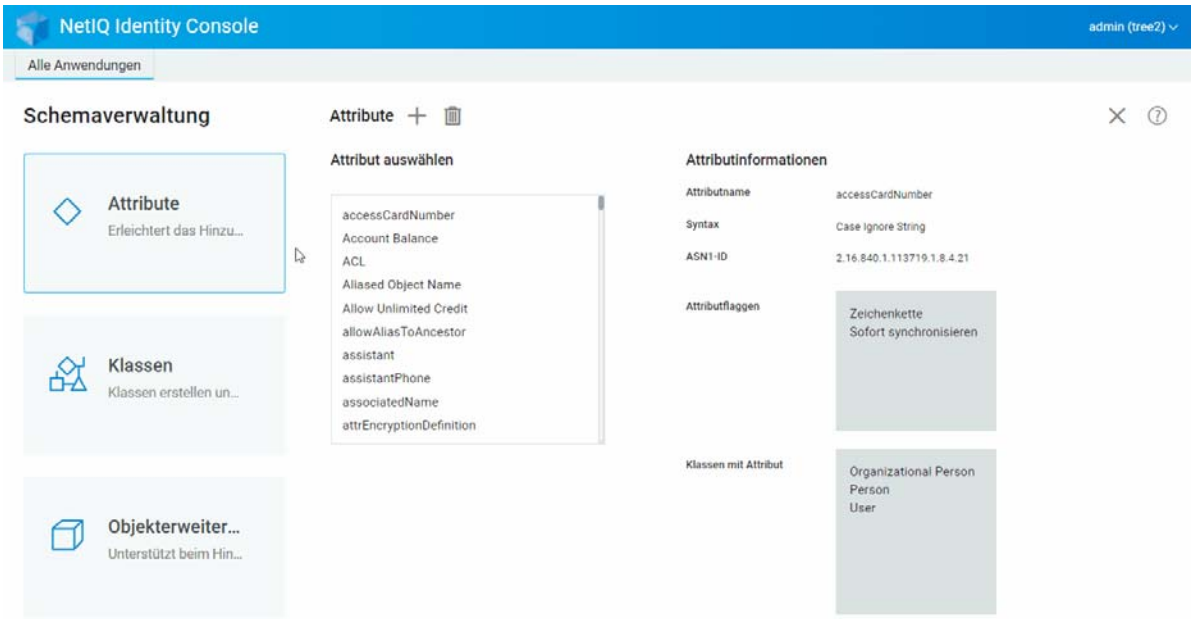


Attributinformationen anzeigen

Sie können die strukturellen Details eines Attributs anzeigen, wie Syntax, Flaggen und Klassen, die das Attribut verwenden. So zeigen Sie die Informationen eines Attributs an:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Schemaverwaltung** und wählen Sie **Attribute** aus.
2. Klicken Sie auf ein beliebiges unter **Attribut auswählen** aufgeführtes Attribut.
3. Rechts im Bildschirm werden die entsprechenden Attributinformationen angezeigt.

Abbildung 10-3 *Attributinformationen anzeigen*



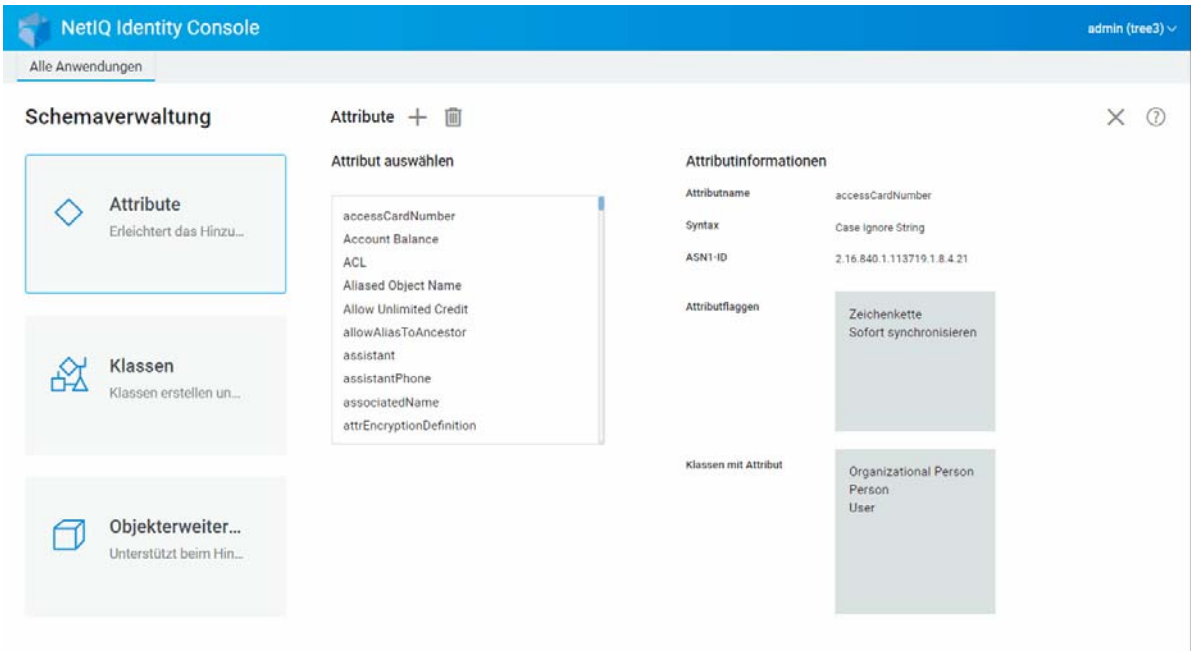
Attribute löschen

Sie können unbenutzte Attribute, die nicht Bestandteil des Basisschemas des eDirectory-Baums sind, löschen. Dies kann hilfreich sein, wenn Sie zwei Verzeichnisbäume zusammengeführt haben oder wenn ein Attribut im Laufe der Zeit veraltet ist. So löschen Sie ein Attribut:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Schemaverwaltung** und wählen Sie **Attribute** aus.
2. Wählen Sie in der Liste **Attribut auswählen** das Attribut aus, das Sie löschen möchten, und klicken Sie auf das Symbol .

   HINWEIS: Das Symbol ist nur aktiv, wenn Sie ein Attribut auswählen, das gelöscht werden kann.
3. Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Abbildung 10-4 *Attribute löschen*



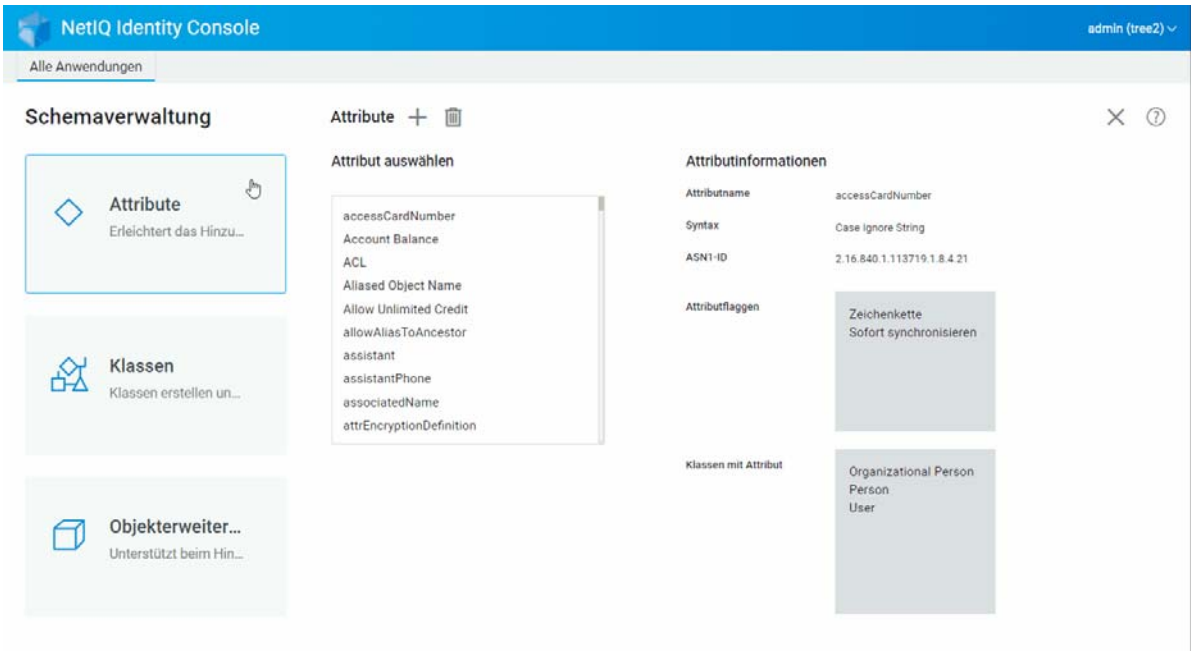
Klassen löschen

Sie können unbenutzte Klassen, die nicht Bestandteil des Basisschemas des eDirectory-Baums sind, löschen. Identity Console verhindert das Löschen von Klassen, die zurzeit in lokale replizierten Partitionen verwendet werden. So löschen Sie eine Klasse:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Schemaverwaltung** und wählen Sie **Klassen** aus.
2. Wählen Sie in der Liste **Klasse auswählen** die Klasse aus, die Sie löschen möchten, und klicken Sie auf das Symbol .

   HINWEIS: Das Symbol ist nur aktiv, wenn Sie eine Klasse auswählen, die gelöscht werden kann.
3. Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Abbildung 10-5 *Klassen löschen*



Objekte erweitern

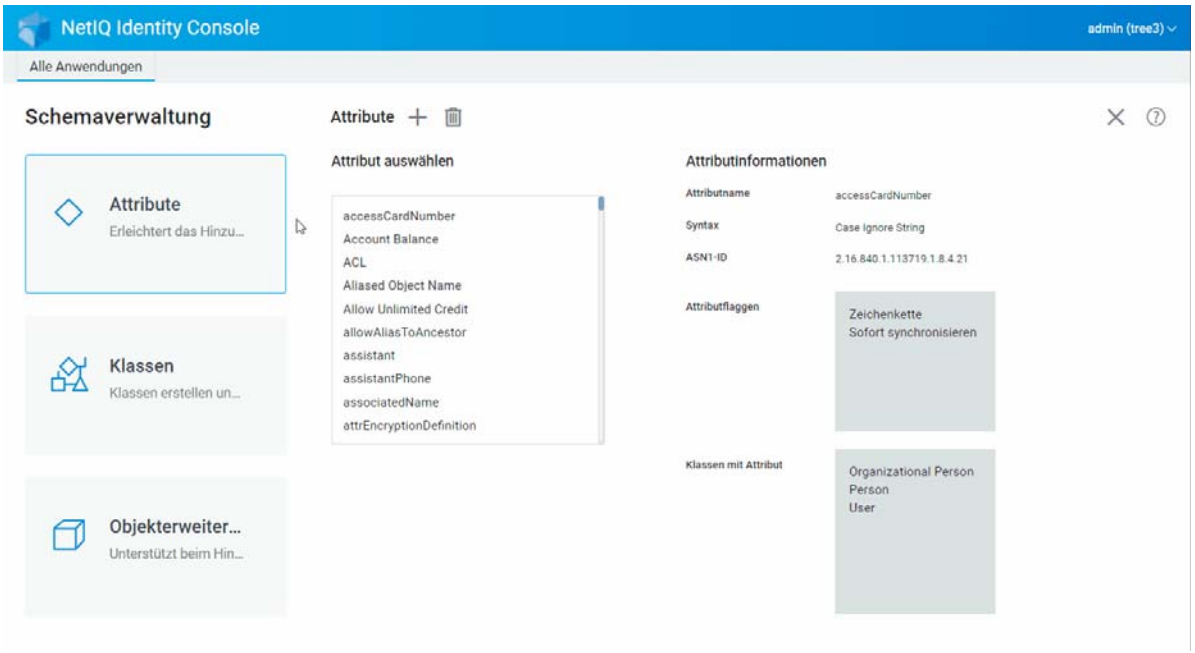
Führen Sie die folgenden Schritte aus, um ein Objekt zu erweitern:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Schemaverwaltung** und wählen Sie **Objekterweiterung** aus.
2. Geben Sie den Objektnamen an oder wählen Sie über die Objektauswahl das zu erweiternde Objekt aus und klicken Sie auf das Symbol .
3. Klicken Sie auf das Symbol und wählen Sie die Zusatzklasse aus. Klicken Sie dann auf **OK**.

   HINWEIS: Wenn ein obligatorisches Attribut mit der ausgewählten Zusatzklasse verknüpft ist, werden Sie im Popup-Fenster **Obligatorische Attribute** aufgefordert, die erforderlichen Werte einzugeben.

   ---
4. Eine Meldung bestätigt das Hinzufügen der Zusatzklasse zum Objekt.
5. Um eine vorhandene Zusatzklasse von einem Objekt zu entfernen, wählen Sie die Klasse aus und klicken Sie auf das Symbol .

Abbildung 10-6 *Objekte erweitern*



11 Revisionsereignisse verwalten

Dieses Kapitel beschreibt die Verwaltung verschiedener Revisionsereignisse mit Identity Console. Mit dieser Funktion können Sie Revisionsereignisse für den NCP-Server aktivieren und deaktivieren.

CEF-Revisionsereignisse konfigurieren

1. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Identity Console an.
2. Wählen Sie **Revision** aus.
3. Wählen Sie den NCP-Server aus, den Sie überwachen möchten, und klicken Sie anschließend auf **OK**.

   HINWEIS: Nachdem Sie CEF-Ereignisse für einen beliebigen NCP-Server zum ersten Mal aktiviert haben, sind standardmäßig bestimmte Ereignisse ausgewählt.

   ---

4. Konfigurieren Sie die CEF-Revisionsereignisse:
   - **Ereigniskonfiguration:** Aktivieren bzw. deaktivieren Sie die folgenden Ereignisse je nach der für die Umgebung erforderlichen Revision:

HINWEIS: Einzelne Ereigniskategorien im Abschnitt der Ereigniskonfiguration sind standardmäßig reduziert. Sie können jede Kategorie erweitern, um einzelne Ereignisse auszuwählen.

Optionen	Beschreibung
Sicherheitsereignisse	Wählen Sie die Sicherheitsereignisse aus, für die Sie Ereignisse protokollieren möchten. Sie können Ereignisse in Bezug auf das Hinzufügen oder Löschen von Mitgliedern, die Unbefugtenerkennung, Passwortänderungen, die Benutzerauthentifizierung usw. protokollieren.
Objektereignisse	Wählen Sie die Objektereignisse aus, für die Sie Ereignisse protokollieren möchten. Sie können Ereignisse in Bezug auf das Löschen, Umbenennen, Verschieben oder Suchen von Objekten protokollieren.
Attributereignisse	Wählen Sie die Attributereignisse aus, für die Sie Ereignisse protokollieren möchten. Sie können Ereignisse zum Lesen und Löschen von Attributen und zum Hinzufügen, Löschen und Vergleichen von Attributwerten protokollieren.
LDAP-Ereignisse	Wählen Sie die LDAP-Ereignisse aus, für die Sie Ereignisse protokollieren möchten.

- **Erweiterte Einstellungen:** In den erweiterten Einstellungen können Sie die folgenden Aktionen ausführen:
  - **Global:** Sie können die globalen Einstellungen für doppelte Einträge auswählen oder löschen.
    - **Keine replizierten Ereignisse senden:** Aktivieren Sie diese Option, um keine Ereignisduplikate bei Replikation von anderen Servern zu erhalten.
  - **Protokollereigniswerte:** Die Ereignisse werden in einer Textdatei protokolliert. Ereigniswerte, deren Größe 768 Byte überschreitet, werden als „große Werte“ betrachtet. Sie können beliebig große Ereignisse protokollieren.
    - **Große Werte protokollieren:** Aktivieren Sie diese Option, um Ereignisse zu protokollieren, deren Größe 768 Byte überschreitet.
    - **Attributwerte protokollieren:** Aktivieren Sie diese Option, um die Attributwerte anzuzeigen. Dies gilt nur für die Ereignisse **Wert hinzufügen** und **Wert löschen**.
    - **Verschlüsselte Attributwerte protokollieren:** Aktivieren Sie diese Option, um die verschlüsselten Attributwerte anzuzeigen. Dies gilt nur für die Ereignisse **Wert hinzufügen** und **Wert löschen**.

    HINWEIS: Wenn das Ereignis größer als 768 Byte ist, wird der Ereigniswert abgeschnitten und in der Protokolldatei gespeichert.

Grundlegendes zu CEF-Ereignistypen

Sie können CEF zur Protokollierung von Ereignissen in den folgenden Kategorien konfigurieren:

- Sicherheit
- Objekte
- Attribute
- LDAP

Sie können den folgenden standardmäßigen Satz an Ereignistypen prüfen:

Kategorie	Ereignistyp
Sicherheit	◆ ACL geändert ◆ Mitglied hinzufügen ◆ Mitglied löschen ◆ Unbefugter Benutzer erkannt ◆ Anmeldung deaktiviert ◆ Anmeldung aktiviert ◆ Anmelden ◆ Sicherheitsäquivalenzen ändern ◆ Revisionskonfiguration ◆ Passwort ändern ◆ Kontoentsperrung ◆ Abmelden ◆ Verbindung ◆ Identität annehmen ◆ Authentifizieren ◆ Passwort überprüfen ◆ Anmeldekonfiguration ändern ◆ Berechtigungsnachweis abfragen
Objekte	◆ Objekt erstellen ◆ Objekt löschen ◆ Objekt umbenennen ◆ Objekt verschieben ◆ DSA-Lesevorgang ◆ Suche
Attribute	◆ Attribut lesen ◆ Attribut löschen ◆ Wert hinzufügen ◆ Wert löschen ◆ Attributwert vergleichen

Kategorie	Ereignistyp
LDAP	◆ LDAP – Bindung ◆ LDAP – Antwort auf Bindung ◆ LDAP – Bindung aufheben ◆ LDAP-Verbindung ◆ LDAP – Suche ◆ LDAP – Antwort auf Suche ◆ LDAP – Antwort auf Sucheintrag ◆ LDAP – Hinzufügen ◆ LDAP – Antwort auf Hinzufügen ◆ LDAP – Vergleich ◆ LDAP – Antwort auf Vergleich ◆ LDAP – Ändern ◆ LDAP – Antwort auf Änderung ◆ LDAP – Löschen ◆ LDAP – Antwort auf Löschen ◆ LDAP – DN ändern ◆ LDAP – Antwort auf DN-Änderung ◆ LDAP – Abbruch ◆ LDAP – Erweiterte Operation ◆ LDAP – Erweiterte Systemoperation ◆ LDAP – Antwort auf erweiterte Operation ◆ LDAP-Serverkonfiguration ändern ◆ Unbekannte LDAP-Operation ◆ LDAP – Passwortänderung

CEF-Revisionsfilterung konfigurieren

Durch Festlegen von Filtern und Ereignisbenachrichtigungen kann CEF melden, wann eine bestimmte Art Ereignis auftritt oder nicht. Je nach Ereignistyp können Sie die Ereignisse auch nach Objektklassen oder Attributen filtern. CEF wertet alle generierten Ereignisse in Bezug auf die konfigurierten Filter auf dem eDirectory-Server aus und protokolliert nur die Ereignisse, die mit den Filterkriterien übereinstimmen.

Dieser Abschnitt enthält Informationen zum Konfigurieren der Systemfilter und Benachrichtigungen.

- „eDirectory-Ereignisse mit Ausschlussfilter filtern“, auf Seite 69
- „CEF-Objektereignisse filtern“, auf Seite 69
- „CEF-Attributereignisse filtern“, auf Seite 70

eDirectory-Ereignisse mit Ausschlussfilter filtern

Klicken Sie auf den Link **Ausschlussfilter**, um das Filtern nach Objektklassen und Attributen zu konfigurieren, für die keine Ereignisse erzeugt werden sollen. Sie können Objektklassen und Attribute auswählen.

So konfigurieren Sie das Filtern von unerwünschten eDirectory-Ereignissen:

1. Wählen Sie in Identity Console auf der Startseite **Revision** aus.
2. Wählen Sie den NCP-Server aus, den Sie überwachen möchten, und klicken Sie anschließend auf **OK**.
3. Wechseln Sie nun zu **Erweiterte Einstellungen** und klicken Sie auf **Ausschlussfilter** im Bereich **Filter**.

   Das Fenster zur CEF-Ausschlussfilterung wird geöffnet.
4. Wählen Sie in der Liste **Verfügbare Objektklassen** die Objektklassen aus, für die keine Ereignisse erfasst werden sollen, und klicken Sie dann auf den Rechtspfeil, um sie zur Liste **Ausgewählte Objektklassen** hinzuzufügen.
5. Wählen Sie in der Liste **Verfügbare Attribute** eine beliebige Anzahl an Attributen aus. Wählen Sie das Attribut aus und klicken Sie auf den Rechtspfeil, um das Attribut zur Liste der ausgewählten Attribute hinzuzufügen.
6. Klicken Sie auf **OK**.

Das CEF-Revisionsmodul wendet den konfigurierten Filter an und generiert für die ausgewählten Objektklassen und Attribute keine Ereignisse.

CEF-Objektereignisse filtern

Sie können die Filterung so konfigurieren, dass Objekte nur nach bestimmten Ereignissen suchen. Wenn Sie beispielsweise benachrichtigt werden möchten, wenn jemand ein Benutzerkonto in eDirectory erstellt, können Sie einen Filter erstellen, für den Sie die Benutzerobjektklasse auswählen, und festlegen, dass Ereignisse in Bezug auf das Erstellen eines neuen Benutzerobjekts protokolliert werden sollen.

Zum Konfigurieren der Kontofilterung klicken Sie auf den Link für die Objektereignisse, wählen Sie die Klasse aus und klicken Sie dann auf **OK**, um die Anwendung zu beenden.

So konfigurieren Sie Filter für Kontoverwaltungsereignisse:

1. Wählen Sie in Identity Console auf der Startseite **Revision** aus.
2. Wählen Sie den NCP-Server aus, den Sie überwachen möchten, und klicken Sie anschließend auf **OK**.
3. Wechseln Sie nun zu **Erweiterte Einstellungen** und klicken Sie auf **Objektereignisse** im Bereich **Filter**.

   Das Fenster zur CEF-Objektfilterung wird geöffnet.
4. Wählen Sie in der Liste **Verfügbare Objektklassen** eine beliebige Objektklasse aus, klicken Sie auf den Rechtspfeil, um die Objektklasse in die Liste **Ausgewählte Objektklassen** zu verschieben, und klicken Sie dann auf **OK**.

Wenn das CEF-Revisionsmodul diesen Filter anwendet, überprüft es alle generierten Ereignisse auf die ausgewählten Objektklassen und protokolliert die entsprechenden Ereignisse.

CEF-Attributereignisse filtern

Klicken Sie auf den Link **Attributereignisse**, um das Filtern für Attributereignisse zu konfigurieren. Wenn Sie beispielsweise benachrichtigt werden möchten, wenn jemand einen neuen Attributwert in eDirectory erstellt, können Sie einen Filter erstellen, um alle Ereignisse in Bezug auf das Hinzufügen eines neuen Werts zu protokollieren.

So konfigurieren Sie das Filtern für Attributereignisse:

1. Wählen Sie in Identity Console auf der Startseite **Revision** aus.
2. Wählen Sie den NCP-Server aus, den Sie überwachen möchten, und klicken Sie anschließend auf **OK**.
3. Wechseln Sie nun zu **Erweiterte Einstellungen** und klicken Sie auf **Attributereignisse** im Bereich **Filter**.

   Das Fenster **Konfiguration der Attributfilterung** wird angezeigt.
4. Wählen Sie in der Liste **Verfügbare Objektklassen** Objektklassen aus, für die Ereignisse erfasst werden sollen, und klicken Sie auf den Rechtspfeil, um sie zur Liste **Ausgewählte Objektklassen** zu verschieben.
5. Wählen Sie in der Liste **Verfügbare Attribute** eine beliebige Anzahl an Attributen für die ausgewählten Objektklassen aus. Wählen Sie das Attribut aus und klicken Sie auf den Rechtspfeil, um das Attribut zur Liste der ausgewählten Attribute hinzuzufügen.

   HINWEIS: Wenn Sie eine Objektklasse auswählen, werden alle Attributereignisse für alle Attribute dieser Objektklasse ausgewählt. In diesem Fall werden alle Attributereignisse für alle Attribute der ausgewählten Objektklassen erfasst.

   ---
6. Klicken Sie auf **OK**.

Wenn der Filter konfiguriert ist, überprüft das CEF-Revisionsmodul die generierten Ereignisse auf alle ausgewählten Objektklassen und Attribute und protokolliert die entsprechenden Ereignisse.

12 Verschlüsselte Attribute verwalten

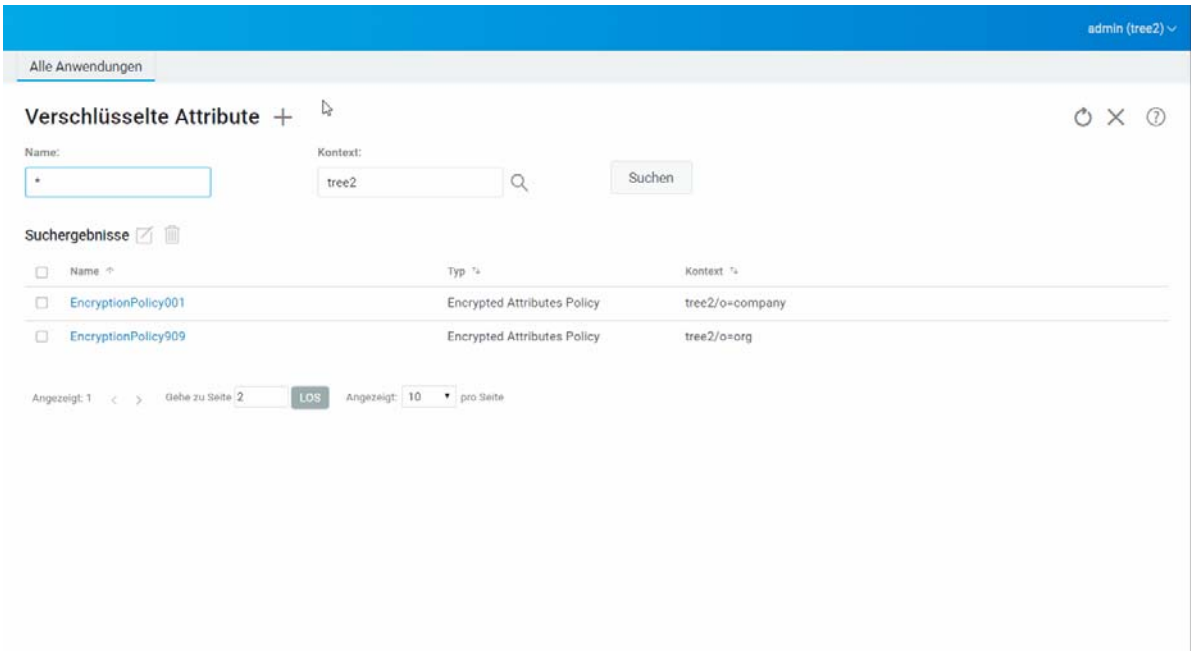
Identity Console kann verschlüsselte Attribute sicher vom eDirectory-Server lesen. Mit Identity Console können Sie verschiedene Richtlinien für diese verschlüsselten Attribute erstellen, ändern oder löschen.

Richtlinie für verschlüsselte Attribute erstellen

So erstellen Sie eine neue Attributrichtlinie:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Verschlüsselte Attribute**.
2. Klicken Sie auf das Symbol +.
3. Geben Sie auf der Seite zum Erstellen einer Richtlinie für verschlüsselte Attribute die folgenden Details ein:
   - Geben Sie den Richtliniennamen an.
   - Geben Sie den Kontext ein oder wählen Sie ihn aus.
   - Wählen Sie den NCP-Server aus.
   - Wählen Sie die Attribute aus.
4. Nachdem Sie alle erforderlichen Details angegeben haben, klicken Sie auf **Beenden**.
5. Eine Meldung bestätigt das Erstellen der Richtlinie.

Abbildung 12-1 *Richtlinie für verschlüsselte Attribute erstellen*

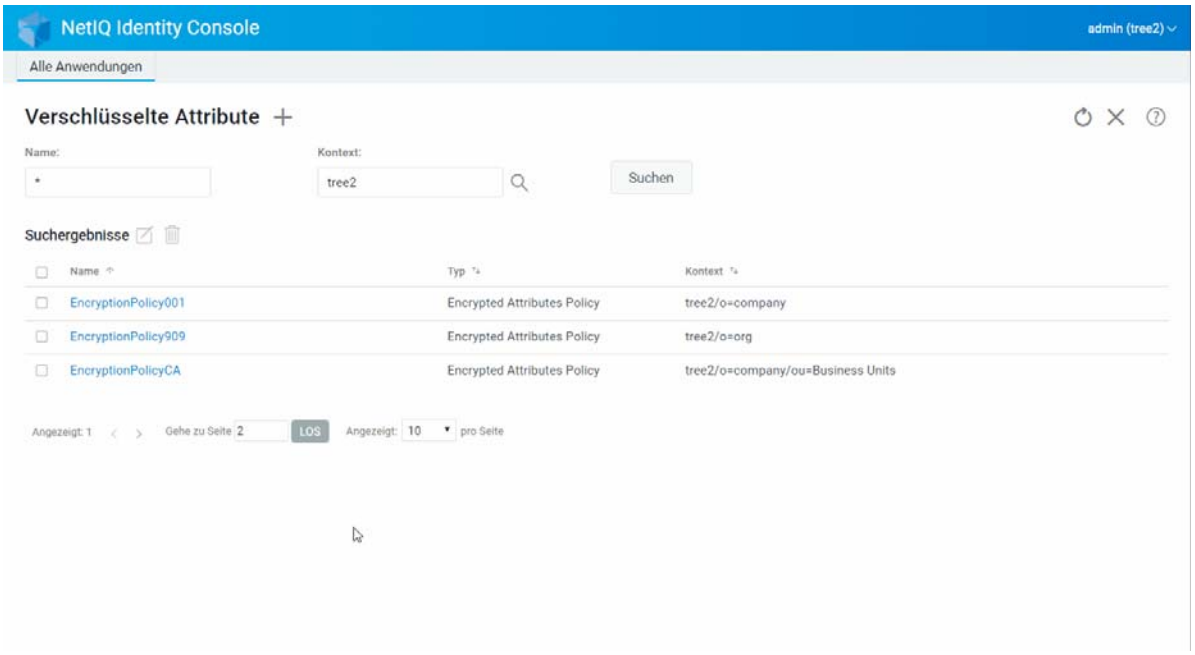


Richtlinie für verschlüsselte Attribute löschen

So löschen Sie eine Richtlinie für verschlüsselte Attribute:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Verschlüsselte Attribute**.
2. Geben Sie den Namen und den Kontext des Attributs an oder verwenden Sie die Suchfunktion, um das Attribut zu finden. Klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie das bzw. die Attribute aus der Liste aus und klicken Sie auf das Symbol 🗑.
4. Eine Meldung bestätigt das Löschen der Richtlinie.

Abbildung 12-2 *Richtlinie für verschlüsselte Attribute löschen*

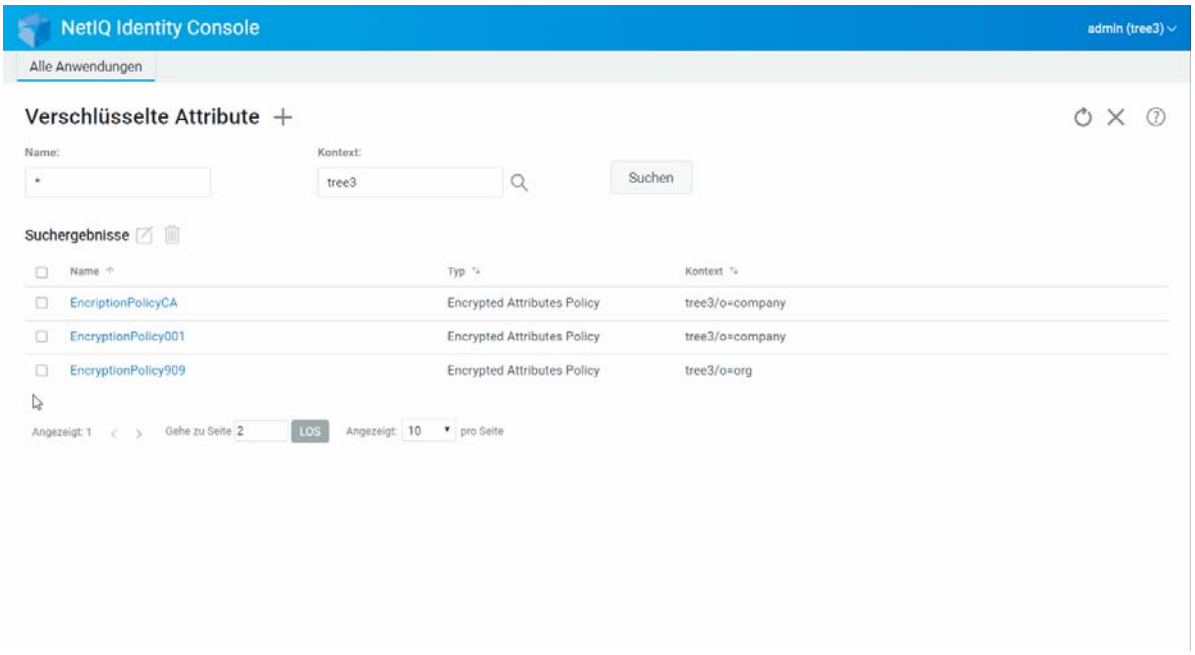


Richtlinie für verschlüsselte Attribute ändern

So ändern Sie eine Richtlinie für verschlüsselte Attribute:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Verschlüsselte Attribute**.
2. Geben Sie den Namen und den Kontext des Objekts ein und klicken Sie auf die Schaltfläche Suchen.
3. Wählen Sie das Attribut aus der Objektliste aus und klicken Sie auf die Schaltfläche .
4. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf die Schaltfläche Speichern.
5. Eine Meldung bestätigt das Ändern der Richtlinie.

Abbildung 12-3 *Richtlinie für verschlüsselte Attribute ändern*



13 Verschlüsselte Replikation verwalten

Um die verschlüsselte Replikation zu aktivieren, müssen Sie eine Partition für die verschlüsselte Replikation konfigurieren. Die Konfigurationseinstellungen werden im Stammobjekt der Partition gespeichert. Sie können die verschlüsselte Replikation ausschließlich auf Partitionsebene aktivieren. Wenn Sie die verschlüsselte Replikation auf Partitionsebene aktivieren, wird die Replikation zwischen allen Replikaten verschlüsselt, die die Partition hosten. Nehmen Sie als Beispiel an, Partition P1 hat die Replikate R1, R2, R3 und R4. Sie können die Replikation zwischen allen Replikaten verschlüsseln.

- „Verschlüsselte Replikation für Partitionen aktivieren“, auf Seite 75

Verschlüsselte Replikation für Partitionen aktivieren

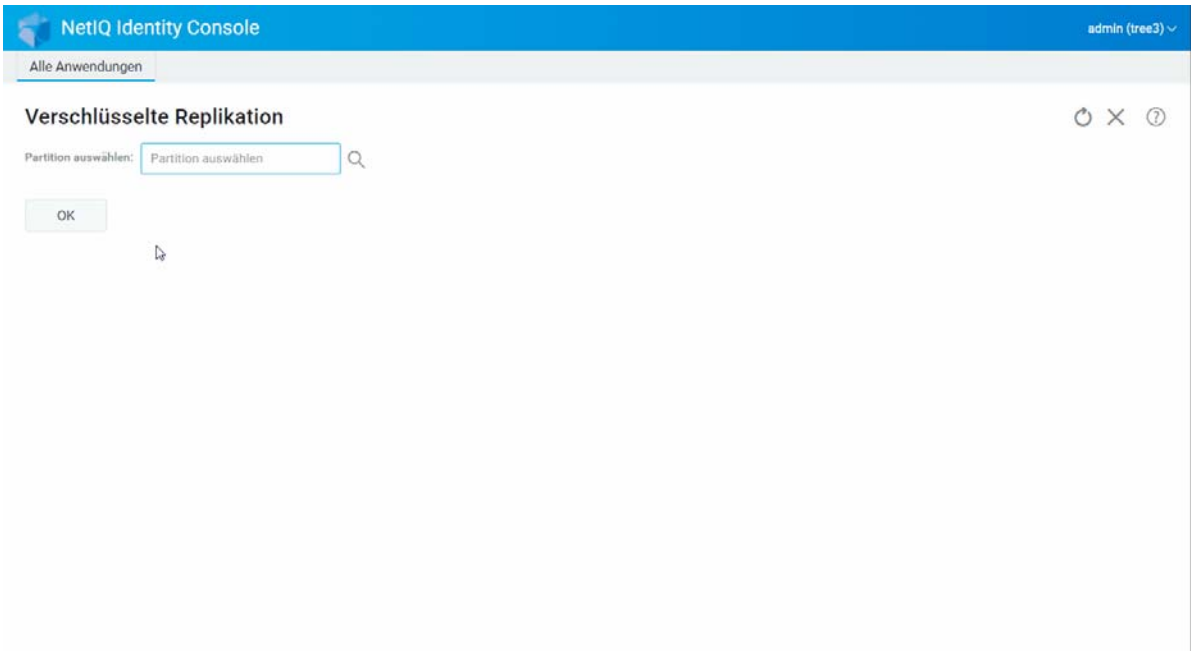
So aktivieren Sie die verschlüsselte Replikation für Partitionen:

HINWEIS: Um die verschlüsselte Replikation für eine Partition zu aktivieren, müssen alle Server, die die Partition hosten, eDirectory 9.2 oder höher ausführen.

---

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Verschlüsselte Replikation**.
2. Geben Sie die Partition ein, für die Sie die verschlüsselte Replikation aktivieren möchten, oder suchen Sie nach der Partition.
3. Vergewissern Sie sich, dass die Option **Verschlüsselte Replikation aktivieren** ausgewählt ist. Wenn Sie die verschlüsselte Replikation für eine Partition deaktivieren, heben Sie die Auswahl dieser Option auf.
4. Klicken Sie auf **Fertigstellen**.
5. Eine Meldung bestätigt das Aktivieren der verschlüsselten Replikation.

Abbildung 13-1 *Verschlüsselte Replikation für Partitionen aktivieren*



14 Partitionen und Reproduktionen verwalten

Mit Partitions- und Reproduktionsvorgängen können Sie den physischen Entwurf und die Verteilung von eDirectory über Ihre Verzeichnisserver verwalten.

Partitionen erstellen logische Unterteilungen des eDirectory-Baums. Wenn Sie beispielsweise eine organisatorische Einheit auswählen und diese als neue Partition anlegen, teilen Sie die organisatorische Einheit und deren untergeordnete Objekte von der übergeordneten Partition ab. Die organisatorische Einheit wird zum Stamm einer neuen Partition. Die Reproduktionen der neuen Partition befinden sich auf demselben Server wie die Reproduktionen der übergeordneten Partition und die Objekte in der neuen Partition gehören zum Stammobjekt der neuen Partition.

Mit dem Partitionsmodul können die folgenden Aufgaben ausgeführt werden:

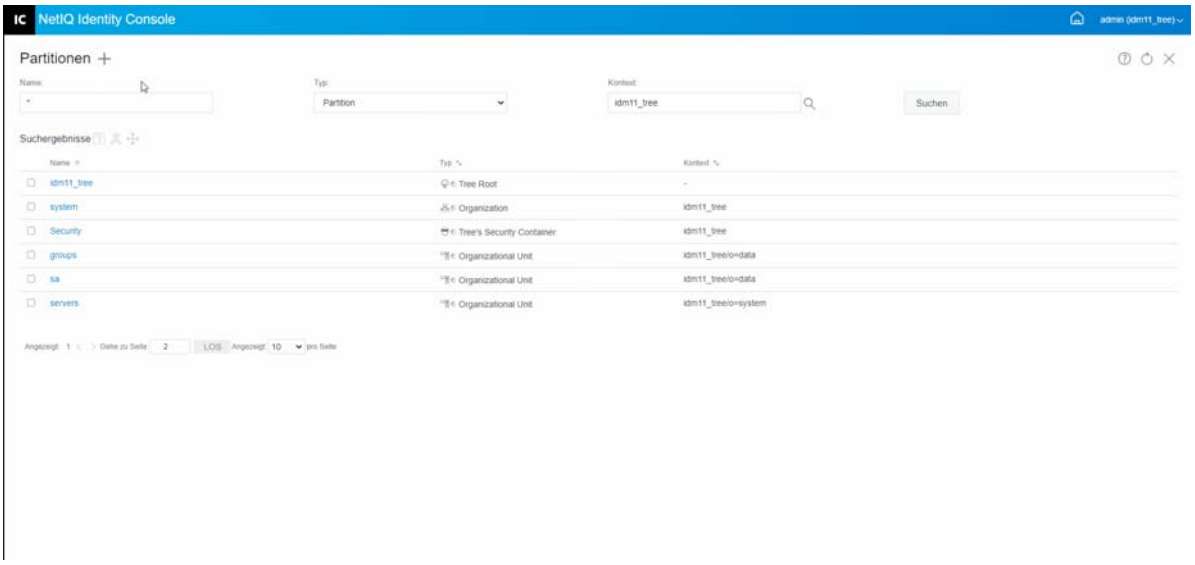
- „Partitionen erstellen“, auf Seite 77
- „Partitionen zusammenführen“, auf Seite 78
- „Partitionen ändern“, auf Seite 79
- „Partitionen verschieben“, auf Seite 80

Partitionen erstellen

So erstellen Sie eine neue Partition:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Partitionsverwaltung**.
2. Klicken Sie auf das Symbol  .
3. Geben Sie auf der Seite „Partition erstellen“ den Container an, der als Stamm der neuen Partition verwendet werden soll, oder verwenden Sie das Objektauswahlsymbol  , um ihn zu suchen, und klicken Sie auf **Erstellen**.
4. Eine Meldung bestätigt das Erstellen der Partition.

Abbildung 14-1 *Neue Partition erstellen*

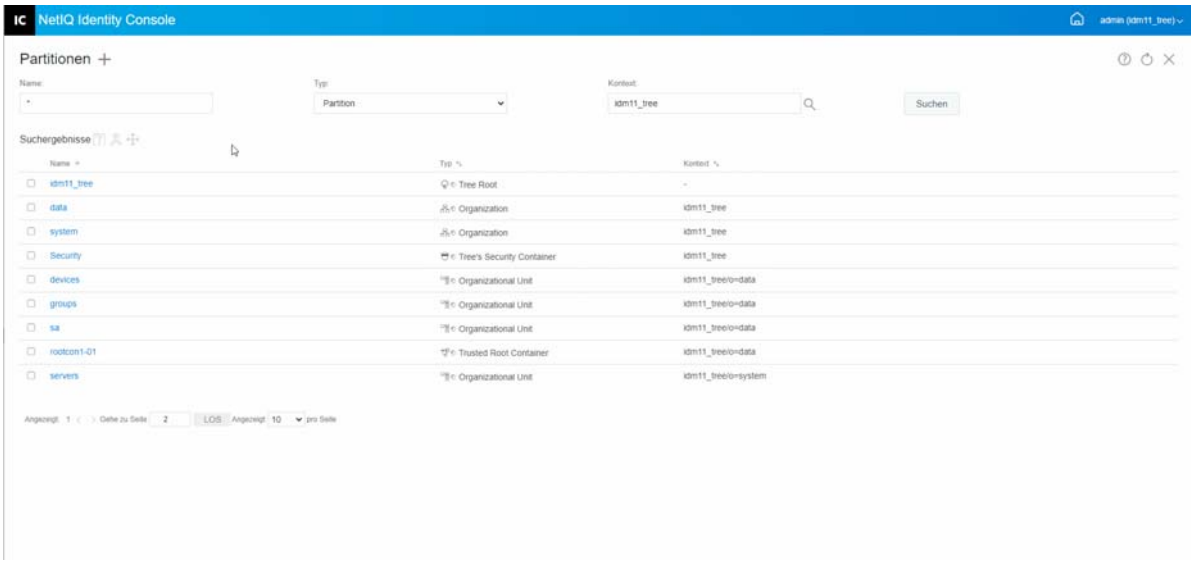


Partitionen zusammenführen

So führen Sie Partitionen mit der übergeordneten Partition zusammen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Partitionsverwaltung**.
2. Geben Sie den Namen, den Typ und den Kontext der Partition an oder suchen Sie sie mithilfe der Suchfunktion. Klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie die Partition aus der Suchliste aus und klicken Sie auf das Symbol  . Klicken Sie dann auf **OK**.
4. Eine Meldung bestätigt das Zusammenführen der Partition.

Abbildung 14-2 *Partitionen zusammenführen*



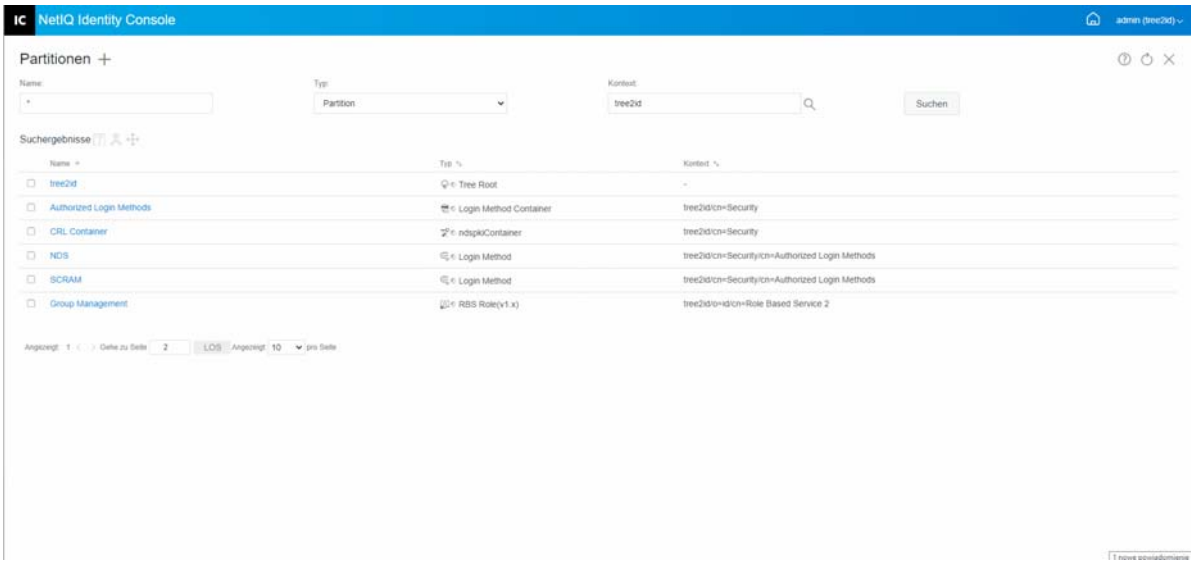
Partitionen ändern

So ändern Sie Partitionen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Partitionsverwaltung**.
2. Geben Sie den Namen, den Typ und den Kontext der Partition an und klicken Sie auf die Schaltfläche Suchen.
3. Wählen Sie die Partition aus der Suchliste aus und klicken Sie auf das Symbol .
4. Klicken Sie unter **Filter** auf die Option **Bearbeiten**, um Replikatfilter und die entsprechenden Klassen und Attribute zu ändern, und klicken Sie dann auf **OK**.

   Wenn Sie im Feld **Typ** die Option **Server** ausgewählt haben, wird die Liste aller Server angezeigt. Durch Klicken auf jeden Server wird eine Liste aller Partitionen auf dem Server angezeigt.
5. Eine Meldung bestätigt die Änderung der Partition.

Abbildung 14-3 *Partitionen ändern*



Partitionen verschieben

Beim Verschieben einer Partition können Sie einen Teilbaum des Verzeichnisbaums verschieben. Dies wird auch als Vorgang zum Entfernen und Hinzufügen bezeichnet. Sie können nur Partitionen verschieben, die nicht über untergeordnete Partitionen verfügen. Wenn untergeordnete Partitionen vorhanden sind, müssen Sie diese Partitionen zuerst zusammenführen, bevor Sie den Vorgang zum Verschieben durchführen können.

Beim Verschieben einer Partition werden alle Verweise auf das Partitionsstammobjekt von eDirectory geändert. Der Eigenname des Objekts bleibt zwar unverändert, doch der vollständige Name des Containers (und aller untergeordneten Ebenen) ändert sich.

HINWEIS: Beim Verschieben einer Partition müssen Sie die Beinhaltungsregeln von eDirectory beachten. Beispiel: Sie können keine organisatorische Einheit direkt unter den Stamm des Verzeichnisbaums verschieben, da die Beinhaltungsregeln fr den Stamm Standort-, Länder- und Organisationsobjekte, aber keine Objektedes Typs "Organisatorische Einheit" zulassen.

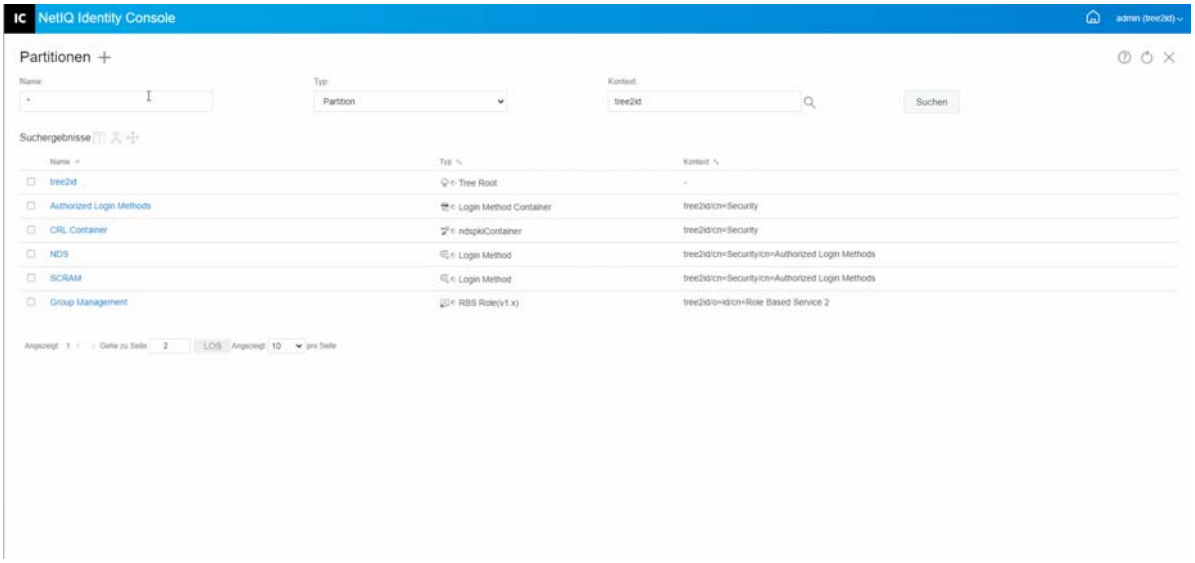
So verschieben Sie eine Partition:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Partitionsverwaltung**.
2. Geben Sie den Namen, den Typ und den Kontext der Partition an und klicken Sie auf die Schaltfläche Suchen.
3. Wählen Sie die Partition aus der Suchliste aus und klicken Sie auf das Symbol ✣.
4. Wählen Sie das Zielcontainerobjekt aus, in das Sie die angegebene Partition verschieben möchten, und klicken Sie auf **OK**.

HINWEIS: Mit **Alias anstelle einer verschobenen Partition erstellen** wird ein Zeiger auf den neuen Speicherort der Partition erstellt. Dadurch können Operationen, die vom alten Standort abhängig sind, ohne Unterbrechungen fortgesetzt werden, bis Sie diese Operationen auf den neuen Standort aktualisieren können. Benutzer können sich im Netzwerk anmelden und Objekte am ursprünglichen Verzeichnisstandort wiederfinden.

5 Eine Meldung bestätigt das erfolgreiche Verschieben der Partition.

Abbildung 14-4 *Partitionen verschieben*



15 Indizes verwalten

Index-Manager ist ein Attribut des Serverobjekts zum Verwalten von Datenbankindizes. Diese Indizes werden von eDirectory verwendet und steigern die Geschwindigkeit von Abfragen erheblich.

NetIQ eDirectory wird mit einem Satz an Indizes geliefert, die grundlegende Abfragefunktionen bereitstellen. Diese Standardindizes können für die folgenden Attribute verwendet werden.

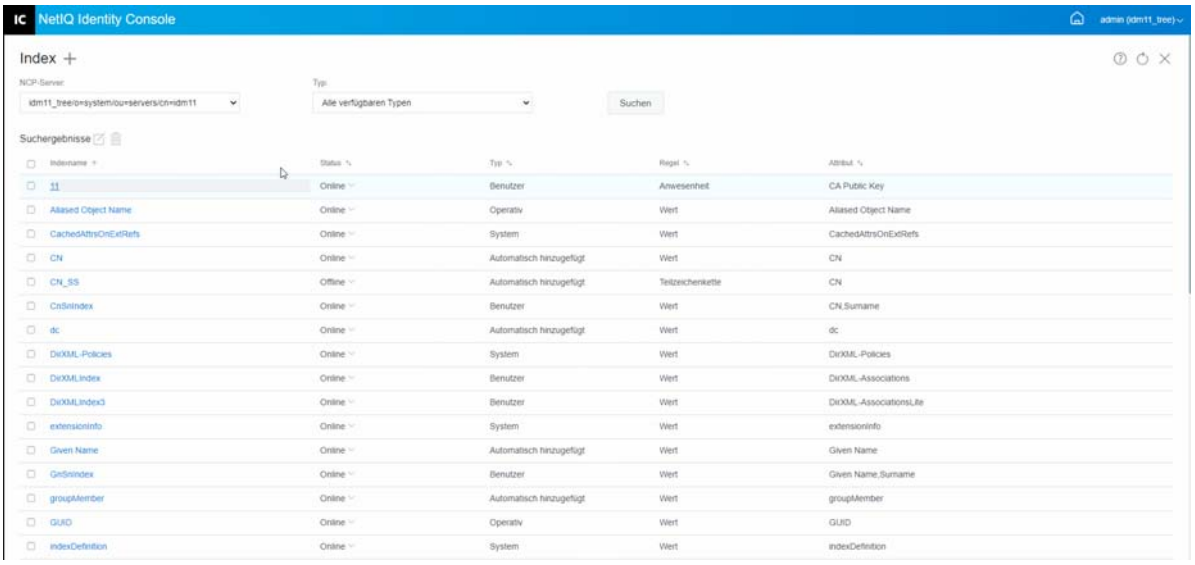
Mit dem Indexmodul können die folgenden Aufgaben ausgeführt werden:

Indizes erstellen

So erstellen Sie einen neuen Index:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Indexverwaltung**.
2. Klicken Sie auf das Symbol +.
3. Geben Sie den Indexnamen ein.
4. Wählen Sie den oder die Server aus der Liste der verfügbaren NCP-Server aus.
5. Wählen Sie das oder die erforderliche(n) Attribut(e) aus.
6. Wählen Sie die Indexregel aus:
   - 6a **Teilzeichenkette:** Es wird eine Übereinstimmung für einen Teil der Attributwertzeichenkette gesucht. Eine Abfrage für einen Nachnamen mit der Teilzeichenkette „der“ würde beispielsweise Treffer für „Derington“, „Anderson“ und „Lauder“ zurückgeben. Teilzeichenketten-Indizes sind hinsichtlich Erstellung und Pflege die ressourcenintensivsten Indizes.
   - 6b **Anwesenheit:** Erfordert lediglich die Anwesenheit eines Attributs und keine bestimmten Attributwerte. Für eine Abfrage zum Ermitteln aller Einträge mit einem Anmeldeskript-Attribut würde ein Anwesenheitsindex verwendet werden.
   - 6c **Wert:** Es wird eine Übereinstimmung mit dem gesamten Attributwert oder dem ersten Teil des Attributwerts gesucht. Die Wertübereinstimmung könnte beispielsweise verwendet werden, um für einen Nachnamen sowohl den Eintrag „Jensen“ als auch alle anderen mit „Jen“ beginnenden Einträge zu finden.
7. Klicken Sie auf die Schaltfläche Erstellen.
8. Eine Meldung bestätigt das Erstellen des Indexes.

Abbildung 15-1 *Neuen Index erstellen*

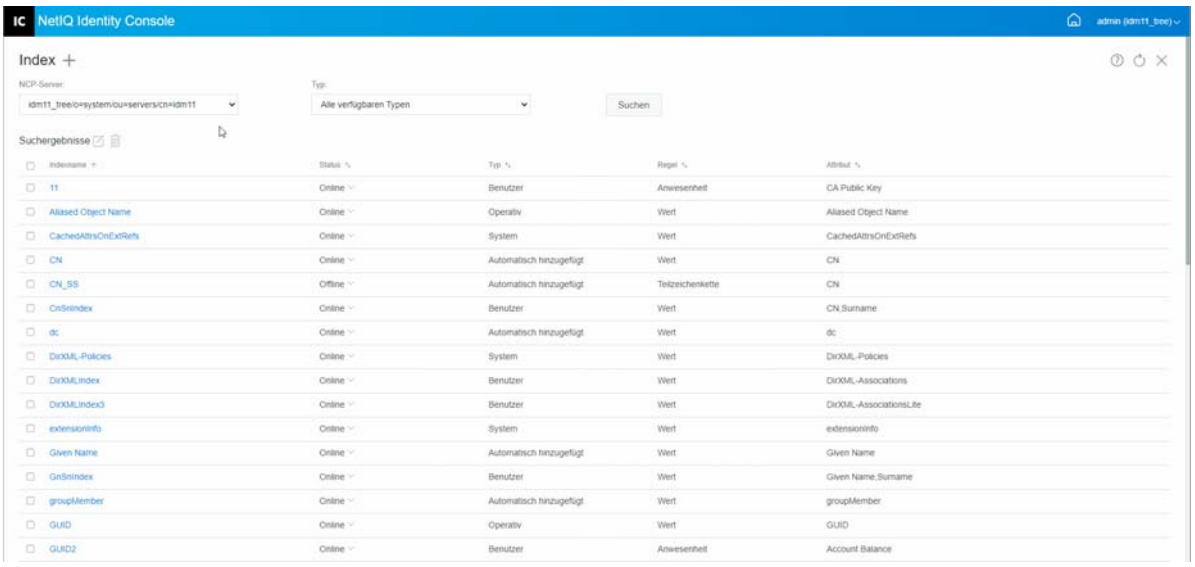


Indizes löschen

So löschen Sie einen Index:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Indexverwaltung**.
2. Wählen Sie den NCP-Server und den Typ des Indexes aus und klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie den Index aus der Suchliste aus und klicken Sie auf das Symbol 🗑.
4. Eine Meldung bestätigt das Löschen des Indexes.

Abbildung 15-2 *Indizes löschen*



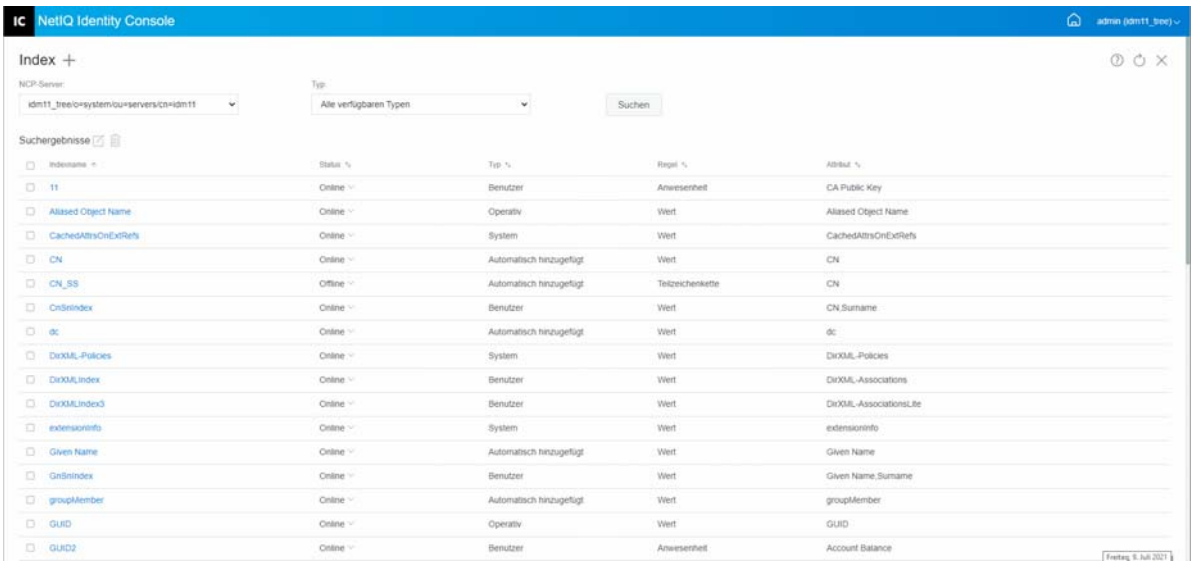
Indizes kopieren

Wenn Sie einen bestimmten Index auf einem Server als nützlich befunden haben und diesen Index auf einem anderen Server verwenden möchten, können Sie die Indexdefinition von einem Server auf einen anderen kopieren. Bei der Überprüfung von Prädikatdaten finden Sie möglicherweise genau das Gegenteil: Ein Index, der auf mehreren Servern einen bestimmten Zweck erfüllte, ist auf einem dieser Server nicht mehr nützlich. In diesem Fall können Sie den Index von dem einzelnen Server löschen, auf dem der Index nicht nützlich ist.

So kopieren Sie einen Index:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Indexverwaltung**.
2. Wählen Sie den NCP-Server und den Typ des Indexes aus und klicken Sie dann auf die Schaltfläche Suchen.
3. Wählen Sie den Index aus der Suchliste aus und klicken Sie auf das Symbol .
4. Wählen Sie den oder die gewünschten NCP-Server aus, auf den/die der Index kopiert werden soll, und klicken Sie auf die Schaltfläche Speichern.
5. Eine Meldung bestätigt die Änderung des Indexes.

Abbildung 15-3 *Indizes kopieren*



Indexstatus ändern

Sie können die Leistung zu Spitzenauslastungszeiten optimieren, indem Sie Indizes vorübergehend offline schalten. Um beispielsweise die Geschwindigkeit während eines Massenladevorgangs zu erhöhen, können Sie alle benutzerdefinierten Indizes vorübergehend anhalten. Da bei jedem

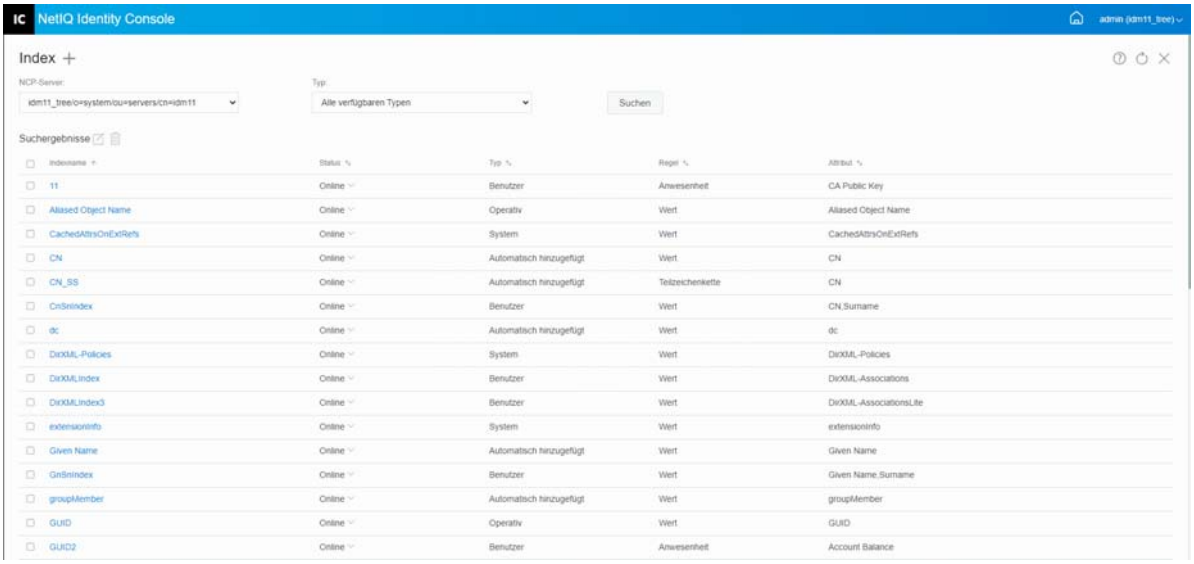
Hinzufügen oder Ändern eines Objekts die definierten Indizes aktualisiert werden müssen, kann das massenhafte Laden von Daten langsam sein, wenn alle Indizes aktiv sind. Nach dem Massenladevorgang können die Indizes wieder online gebracht werden.

So legen Sie einen Index als offline fest:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Indexverwaltung**.
2. Wählen Sie den NCP-Server und den Typ des Indexes aus und klicken Sie dann auf die Schaltfläche Suchen.
3. Klicken Sie in der Liste der Indizes auf die Dropdown-Liste für den **Status**. Ein Index kann einen der folgenden Status haben:
   - **Online:** Index wird aktuell ausgeführt.
   - **Offline:** Ausgesetzt. Der Index kann erneut gestartet werden.

HINWEIS: Der Status von Indizes des Typs „System“ oder „Operativ“ kann nicht geändert werden. Indizes dieses Typs können auch nicht gelöscht werden.

Abbildung 15-4 *Indexstatus auf „Offline“ festlegen*



16 LDAP-Objekte konfigurieren

Bei einer eDirectory-Installation werden ein LDAP-Serverobjekt und ein LDAP-Gruppenobjekt erstellt. Die Standardkonfiguration für LDAP-Services befindet sich im Verzeichnis dieser beiden Objekte. Sie können die Standardkonfiguration mit der LDAP-Verwaltungsaufgabe in Identity Console ändern.

Das LDAP-Serverobjekt stellt serverspezifische Konfigurationsdaten dar. Das LDAP-Gruppenobjekt enthält jedoch Konfigurationsinformationen, die bequem für mehrere LDAP-Server gemeinsam genutzt werden können. Dieses Objekt stellt allgemeine Konfigurationsdaten bereit und stellt eine Gruppe von LDAP-Servern dar. Die Server verfügen über gemeinsame Daten.

Sie können mehrere LDAP-Serverobjekte mit einem LDAP-Gruppenobjekt verknüpfen. Alle verknüpften LDAP-Server erhalten dann ihre serverspezifische Konfiguration von ihrem LDAP-Serverobjekt, aber erhalten allgemeine oder freigegebene Informationen vom LDAP-Gruppenobjekt.

Mit dem LDAP-Modul können die folgenden Aufgaben ausgeführt werden:

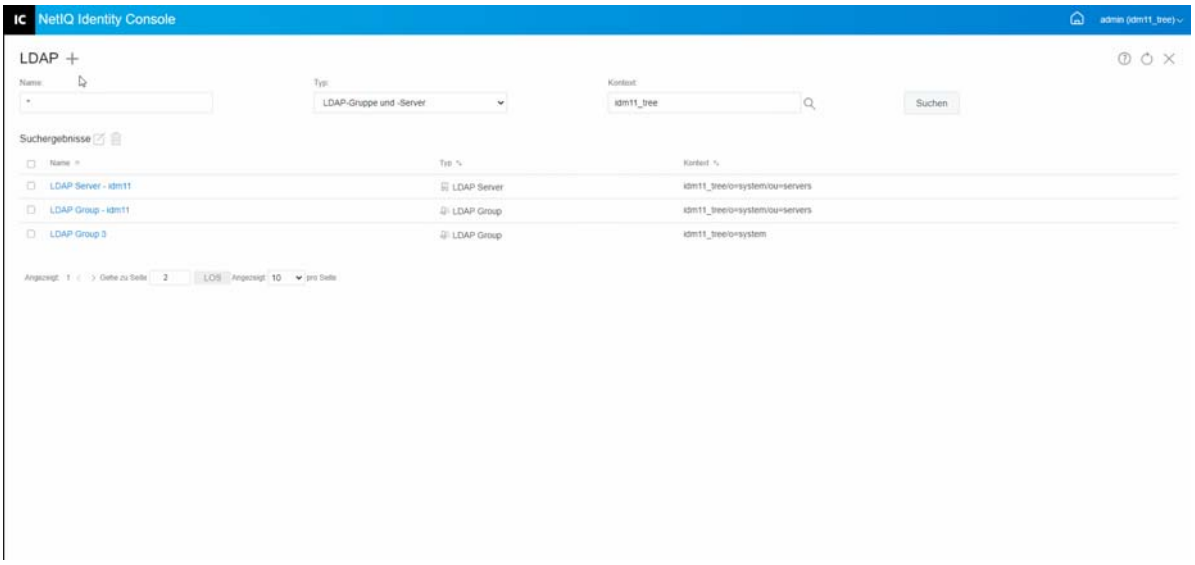
- „LDAP-Objekte erstellen“, auf Seite 87
- „LDAP-Objekte löschen“, auf Seite 88
- „LDAP-Objekte ändern“, auf Seite 89

LDAP-Objekte erstellen

So erstellen Sie ein neues LDAP-Objekt:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **LDAP-Konfiguration**.
2. Klicken Sie auf das Symbol +.
3. Geben Sie auf der Seite „LDAP-Objekt erstellen“ den Namen, den Typ und den Kontext an oder verwenden Sie das Symbol „Kontext suchen“ , um den Kontext zu suchen, und klicken Sie dann auf **Erstellen**.
4. Eine Meldung bestätigt das Erstellen des LDAP-Objekts.

Abbildung 16-1 *Neues LDAP-Objekt erstellen*

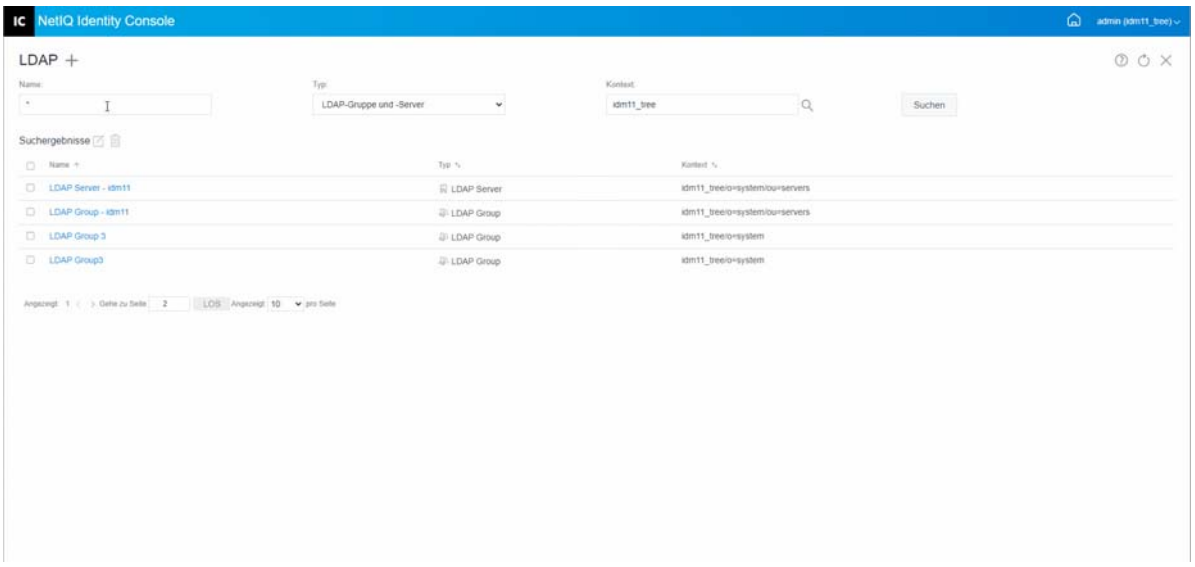


LDAP-Objekte löschen

So löschen Sie LDAP-Objekte:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **LDAP-Konfiguration**.
2. Geben Sie den Namen, den Typ und den Kontext des LDAP-Objekts an und klicken Sie auf die Schaltfläche Suchen.
3. Wählen Sie das oder die LDAP-Objekt(e) aus der Suchliste aus und klicken Sie auf das Symbol 🗑.
4. Eine Meldung bestätigt das Löschen des LDAP-Objekts.

Abbildung 16-2 *LDAP-Objekte löschen*

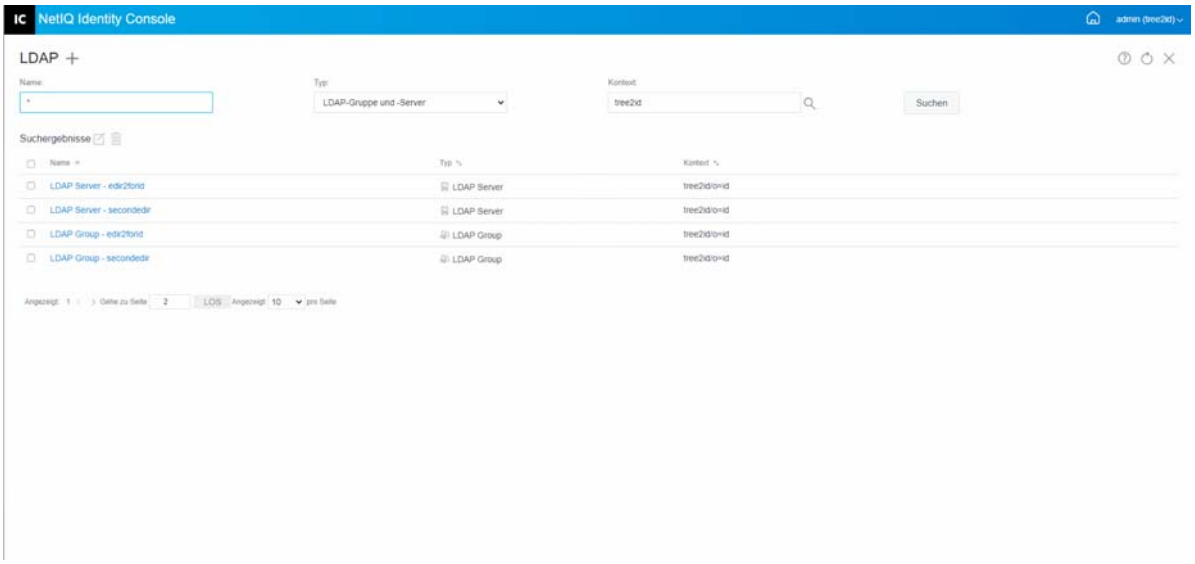


LDAP-Objekte ändern

So ändern Sie LDAP-Objekte:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **LDAP-Konfiguration**.
2. Geben Sie den Namen, den Typ und den Kontext des LDAP-Objekts ein und klicken Sie auf die Schaltfläche Suchen.
3. Wählen Sie das LDAP-Objekt aus der Suchliste aus und klicken Sie auf das Symbol .
4. Ändern Sie je nach Bedarf die Attribute und Informationen für das jeweilige LDAP-Objekt und klicken Sie auf die Schaltfläche Speichern. Weitere Informationen zu den Attributen für LDAP-Objekte finden Sie unter Configuring LDAP Server and LDAP Group Objects on Linux (Konfigurieren von LDAP-Server- und LDAP-Gruppenobjekten unter Linux) im *NetIQ eDirectory Administration Guide* (NetIQ eDirectory-Administrationshandbuch).
5. Eine Meldung bestätigt die Änderung des LDAP-Objekts.

Abbildung 16-3 *LDAP-Objekte ändern*



17 Zertifikate verwalten

NetIQ Certificate Server wird automatisch installiert, wenn Sie eDirectory installieren. Certificate Server stellt Services für Public-Key-Verschlüsselungsverfahren bereit, die in eDirectory integriert sind. Anhand dieser Schlüssel können Sie sowohl Benutzer- als auch Serverzertifikate erstellen, ausstellen und verwalten. Diese Services ermöglichen den Schutz vertraulicher Daten bei der Übertragung über öffentliche Kommunikationskanäle, z. B. über das Internet.

HINWEIS: Wenn Sie das Zertifikatverwaltungsmodul mit Identity Console verwenden möchten, müssen Sie Ihren eDirectory-Server auf 9.2.4 HF2 aufrüsten.

Mit Identity Console können Sie die folgenden Zertifikatverwaltungsaufgaben ausführen:

- „Zertifizierungsstelle verwalten“, auf Seite 91
- „Serverzertifikate verwalten“, auf Seite 95
- „Benutzerzertifikate verwalten“, auf Seite 98
- „Herkunftsverbürgung und Container verwalten“, auf Seite 100
- „Standardserverzertifikatsobjekte erstellen“, auf Seite 103
- „Zertifikate mit öffentlichem Schlüssel ausstellen“, auf Seite 104
- „SAS Service-Objekt verwalten“, auf Seite 108

Zertifizierungsstelle verwalten

Standardmäßig erstellt der NetIQ Certificate Server-Installationsprozess die Organisationszertifizierungsstelle für Sie. Sie werden aufgefordert, einen Namen für die Organisationszertifizierungsstelle anzugeben. Wenn Sie auf „Fertigstellen“ klicken, wird die Organisationszertifizierungsstelle mit den Standardparametern erstellt und im Sicherheitscontainer platziert. Wenn Sie mehr Kontrolle über die Erstellung der Organisationszertifizierungsstelle haben möchten, können Sie die Organisationszertifizierungsstelle im Identity Console-Portal manuell erstellen. Wenn Sie die Organisationszertifizierungsstelle löschen, müssen Sie sie neu erstellen.

Mit dem Zertifizierungsstellenmodul können Sie die folgenden Aufgaben ausführen:

- „Organisationszertifizierungsstellenobjekte erstellen“, auf Seite 92
- „Organisationszertifizierungsstellen sichern“, auf Seite 92
- „Organisationszertifizierungsstelle wiederherstellen“, auf Seite 93
- „Zertifikate der Organisationszertifizierungsstelle bestätigen“, auf Seite 94
- „Zertifikate der Organisationszertifizierungsstelle ersetzen“, auf Seite 94
- „Zertifikate der Organisationszertifizierungsstelle widerrufen“, auf Seite 94

Organisationszertifizierungsstellenobjekte erstellen

Führen Sie die folgenden Schritte aus, um ein Organisationszertifizierungsstellenobjekt zu erstellen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **ZS-Verwaltung**.
2. Wenn kein Organisationszertifizierungsstellenobjekt vorhanden ist, werden das Dialogfeld „Create an Organizational Certificate Authority Object“ (Organisationszertifizierungsstellenobjekt erstellen) und der entsprechende Assistent zum Erstellen des Objekts geöffnet. Befolgen Sie die Aufforderungen, um das Objekt zu erstellen.

   HINWEIS: Stellen Sie sicher, dass der hier angegebene Dateipfad für die Zertifikatswiderrufsliste den eDirectory-Installationspfad beachtet.
3. Nachdem Sie die Erstellung der Zertifizierungsstelle abgeschlossen haben, empfiehlt es sich, eine Sicherung des öffentlichen/privaten Schlüsselpaars der Zertifizierungsstelle zu erstellen und diese an einem sicheren Ort zu speichern. Weitere Informationen finden Sie im „Organisationszertifizierungsstellen sichern“, auf Seite 92.

Organisationszertifizierungsstellen sichern

Es wird empfohlen, den privaten Schlüssel und die Zertifikate der Organisationszertifizierungsstelle für den Fall zu sichern, dass auf dem Hostserver der Organisationszertifizierungsstelle ein nicht behebbarer Fehler auftritt. Sollte ein Fehler auftreten, können Sie die Organisationszertifizierungsstelle mithilfe der Sicherungsdatei auf einem beliebigen Server im Baum wiederherstellen.

HINWEIS: Die Möglichkeit zum Sichern einer Organisationszertifizierungsstelle ist nur für Organisationszertifizierungsstellen verfügbar, die mit Certificate Server 9.0 oder höher erstellt wurden. In früheren Versionen von Certificate Server wurde der private Schlüssel der Organisationszertifizierungsstelle so erstellt, dass ein Exportieren unmöglich war.

Die Sicherungsdatei enthält den privaten Schlüssel der Zertifizierungsstelle, das eigensignierte Zertifikat, das Zertifikat mit öffentlichem Schlüssel und mehrere andere Zertifikate, die für den Betrieb erforderlich sind. Diese Informationen werden im PKCS#12-Format (auch als PFX bezeichnet) gespeichert.

Die Organisationszertifizierungsstelle sollte gesichert werden, wenn sie ordnungsgemäß funktioniert.

Führen Sie die folgenden Schritte aus, um die Organisationszertifizierungsstelle zu sichern:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **ZS-Verwaltung**.
2. Klicken Sie auf die Registerkarte **Zertifikate**.
3. Wählen Sie entweder das **eigensignierte Zertifikat** oder das **Zertifikat mit öffentlichem Schlüssel** aus. Beide Zertifikate werden während des Sicherungsvorgangs in die Datei geschrieben. Es wird empfohlen, das eigensignierte Zertifikat für RSA- und ECDSA-Zertifikate separat auszuwählen.
4. Klicken Sie auf das Symbol  .

5 Wählen Sie das Exportieren des privaten Schlüssels, geben Sie ein Passwort mit mindestens sechs alphanumerischen Zeichen an, das zum Verschlüsseln der PFX-Datei verwendet werden soll, und wählen Sie PKCS12 als Exportformat aus. Klicken Sie dann auf **OK**.

6 Die verschlüsselte Sicherungsdatei wird an den angegebenen Speicherort geschrieben. Sie kann nun an einem sicheren Speicherort gespeichert werden, sodass sie im Notfall zur Verfügung steht.

Organisationszertifizierungsstelle wiederherstellen

Wenn das Organisationszertifizierungsstellenobjekt gelöscht oder beschädigt wurde oder auf dem Hostserver der Organisationszertifizierungsstelle ein nicht behebbarer Fehler aufgetreten ist, kann die Organisationszertifizierungsstelle mithilfe einer Sicherungsdatei, die wie unter „Organisationszertifizierungsstellen sichern“, auf Seite 92 beschrieben erstellt wurde, wiederhergestellt werden.

Führen Sie die folgenden Schritte aus, um die Organisationszertifizierungsstelle wiederherzustellen:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **ZS-Verwaltung**.

2 Klicken Sie oben im Bildschirm auf ↑↓ (neben **Verwaltung der Zertifizierungsstelle**), um die vorhandene Organisationszertifizierungsstelle zu löschen.

3 Sie werden nun aufgefordert, eine neue Organisationszertifizierungsstelle zu konfigurieren. Das Dialogfeld "Organisatorische Zertifikatsautorität erstellen" wird geöffnet, und der entsprechende Assistent zum Erstellen des Objekts wird gestartet.

4 Geben Sie im Dialogfeld zur Erstellung den Server, auf dem die Organisationszertifizierungsstelle gehostet werden soll, und den Namen des Organisationszertifizierungsstellenobjekts an.

5 Wählen Sie **Importieren** aus.

6 Wählen Sie sowohl RSA- als auch ECDSA-Zertifikate aus. Certificate Server erfordert, dass beide Zertifikate denselben Antragstellernamen haben. Certificate Server unterstützt jedoch nicht das Importieren externer eigensignierter Zertifizierungsstellenzertifikate. Sie können jedoch untergeordnete Zertifizierungsstellenzertifikate importieren.

7 Wählen Sie in den folgenden Bildschirmen durch Durchsuchen den Namen der Datei für die RSA- und ECDSA-Zertifikate aus.

8 Geben Sie das Passwort ein, das beim Erstellen der Sicherung zum Verschlüsseln der Datei verwendet wurde, und klicken Sie auf **OK**.

9 Der private Schlüssel und die Zertifikate der Organisationszertifizierungsstelle wurden jetzt wiederhergestellt und die Zertifizierungsstelle ist wieder voll funktionsfähig. Die Datei kann nun für die zukünftige Verwendung wieder gespeichert werden.

Zertifikate der Organisationszertifizierungsstelle bestätigen

Wenn Sie ein Problem mit einem Zertifikat vermuten oder der Meinung sind, dass es möglicherweise nicht mehr gültig ist, können Sie das Zertifikat mithilfe von Identity Console bestätigen. Jedes Zertifikat im eDirectory-Baum kann bestätigt werden, auch Zertifikate, die von externen Zertifizierungsstellen ausgestellt wurden.

Der Zertifikatbestätigungsprozess umfasst mehrere Überprüfungen der Daten im Zertifikat sowie der Daten in der Zertifikatskette. Eine Zertifikatskette besteht aus einem Stammzertifizierungsstellenzertifikat und optional aus den Zertifikaten einer oder mehrerer Zwischenzertifizierungsstellen.

So bestätigen Sie ein Zertifikat:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **ZS-Verwaltung**.
2. Klicken Sie auf die Registerkarte **Zertifikate**.
3. Wählen Sie entweder das **eigensignierte Zertifikat** oder das **Zertifikat mit öffentlichem Schlüssel** aus.
4. Klicken Sie auf , um die ausgewählten Zertifizierungsstellenzertifikate zu bestätigen.

Zertifikate der Organisationszertifizierungsstelle ersetzen

Wenn die Zertifikate aus einem beliebigen Grund beschädigt wurden oder ungültig geworden sind oder Sie einfach die vorhandenen Zertifikate ersetzen möchten, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **ZS-Verwaltung**.
2. Klicken Sie auf die Registerkarte **Zertifikate**.
3. Wählen Sie entweder das **eigensignierte Zertifikat** oder das **Zertifikat mit öffentlichem Schlüssel** aus.
4. Klicken Sie auf , um das ausgewählte Zertifizierungsstellenzertifikat zu ersetzen.
5. Importieren Sie ein Zertifizierungsstellenzertifikat im Format `.pfx` oder `.p12` und geben Sie ein Passwort zum Verschlüsseln des privaten Schlüssels an.
6. Klicken Sie auf **OK**.

Zertifikate der Organisationszertifizierungsstelle widerrufen

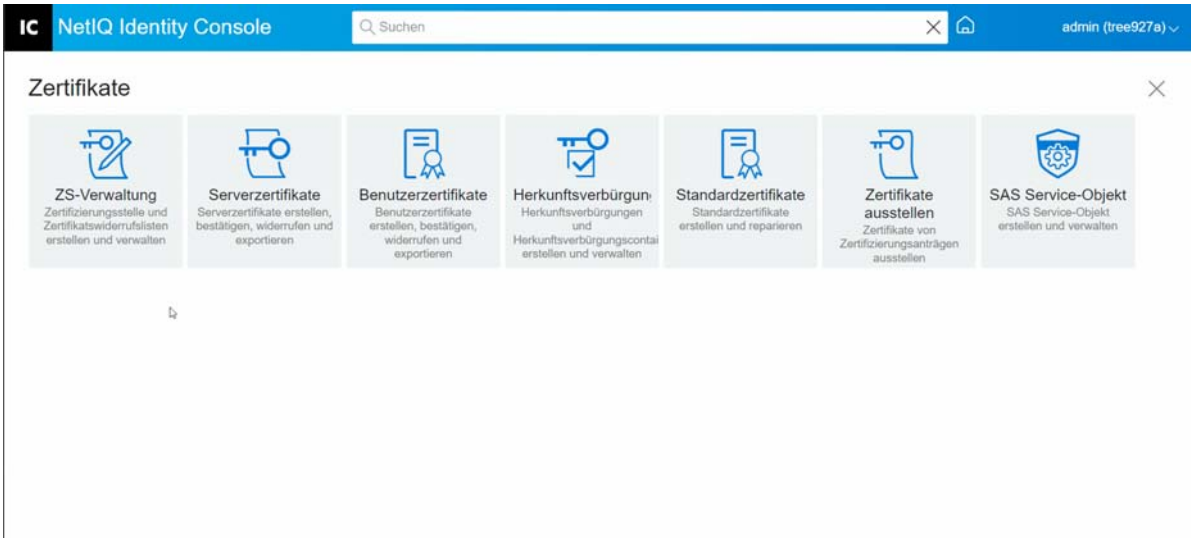
So widerrufen Sie ein Zertifikat:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **ZS-Verwaltung**.
2. Klicken Sie auf die Registerkarte **Zertifikate**.
3. Wählen Sie entweder das **eigensignierte Zertifikat** oder das **Zertifikat mit öffentlichem Schlüssel** aus.
4. Klicken Sie auf das Symbol .
5. Lesen Sie die Hinweise zum Risiko, das mit dem Widerruf von Serverzertifikaten verbunden ist.

6 Wählen Sie aus der Dropdown-Liste einen gültigen Grund für den Widerruf aus, wählen Sie das Datum der Ungültigkeit aus und geben Sie beliebige weitere Kommentare an.

7 Klicken Sie auf **OK**, um das Widerrufen abzuschließen.

Abbildung 17-1 *Zertifizierungsstelle verwalten*



Serverzertifikate verwalten

Mit dem Serverzertifikatverwaltungsmodul kann der Administrator die folgenden Aufgaben ausführen:

- „Serverzertifikatsobjekte erstellen“, auf Seite 95
- „Serverzertifikatsobjekte exportieren“, auf Seite 96
- „Serverzertifikatsobjekte bestätigen“, auf Seite 96
- „Serverzertifikatsobjekte ersetzen“, auf Seite 96
- „Serverzertifikatsobjekte widerrufen“, auf Seite 97
- „Serverzertifikatsobjekte löschen“, auf Seite 97

Serverzertifikatsobjekte erstellen

Führen Sie die folgenden Schritte aus, um ein Serverzertifikatsobjekt zu erstellen:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Serverzertifikate**.

2 Klicken Sie auf das Symbol +.

3 Geben Sie auf der Seite **Serverzertifikat erstellen** einen Namen in das Feld **Kurzname** ein, geben Sie einen Server an und wählen Sie eine der folgenden Optionen aus:

- **Standard (Standardparameter):** Ermöglicht das Erstellen eines Standardserverzertifikatsobjekts vom Typ RSA oder ECDSA.
- **Benutzerdefiniert (Benutzer gibt Parameter an):** Ermöglicht die Angabe benutzerdefinierter Parameter für das Serverzertifikatsobjekt.

- **Importieren (Erlaubt die Bereitstellung der Schlüssel und Zertifikate in einer PKCS12-Datei):** Ermöglicht das Importieren einer PKCS12-Datei im Format `.pfx` oder `.p12`.

4 Klicken Sie nach der Angabe der Parameter auf **Weiter**, um die Zusammenfassung des Zertifikats zu überprüfen.

5 Klicken Sie im Bildschirm **Zusammenfassung** auf **OK**, um ein Serverzertifikatsobjekt zu erstellen.

Serverzertifikatsobjekte exportieren

Führen Sie die folgenden Schritte aus, um Serverzertifikatsobjekte zu exportieren:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Serverzertifikate**.

2 Wählen Sie in der Dropdown-Liste den geeigneten Server aus.

3 Wählen Sie das geeignete Serverzertifikat aus der Liste aus und klicken Sie auf das Symbol .

4 Aktivieren Sie im nächsten Bildschirm das Kontrollkästchen **Privaten Schlüssel exportieren** und geben Sie ein Passwort zum Schutz des privaten Schlüssels an. Bestätigen Sie das Passwort und wählen Sie das Exportformat aus.

HINWEIS: Serverzertifikate können nur im PKCS12-Format exportiert werden.

---

5 Klicken Sie auf **OK**, um das Serverzertifikatsobjekt zu exportieren.

Serverzertifikatsobjekte bestätigen

Führen Sie die folgenden Schritte aus, um ein Serverzertifikatsobjekt zu bestätigen:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Serverzertifikate**.

2 Wählen Sie in der Dropdown-Liste den geeigneten Server aus.

3 Wählen Sie das geeignete Serverzertifikat aus der Liste aus und klicken Sie auf das Symbol .

4 Eine Meldung bestätigt die erfolgreiche Bestätigung des Serverzertifikatsobjekts.

Serverzertifikatsobjekte ersetzen

Wenn die Serverzertifikate aus einem beliebigen Grund beschädigt wurden oder ungültig geworden sind oder Sie einfach die vorhandenen Standardzertifikate ersetzen möchten, führen Sie die folgenden Schritte aus:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Serverzertifikate**.

2 Wählen Sie in der Dropdown-Liste den geeigneten Server aus.

3 Wählen Sie das geeignete Serverzertifikat aus der Liste aus und klicken Sie auf das Symbol .

4 Lesen Sie die Hinweise zum Risiko, das mit dem Ersetzen von Serverzertifikaten verbunden ist, und klicken Sie auf **OK**.

5 Wählen Sie im nächsten Bildschirm durch Durchsuchen das neue Serverzertifikat im Format `.pfx` oder `.p12` aus und geben Sie ein Passwort an.

6 Klicken Sie auf **OK**, um das Serverzertifikat zu ersetzen.

Serverzertifikatsobjekte widerrufen

Führen Sie die folgenden Schritte aus, um ein Serverzertifikatsobjekt zu widerrufen:

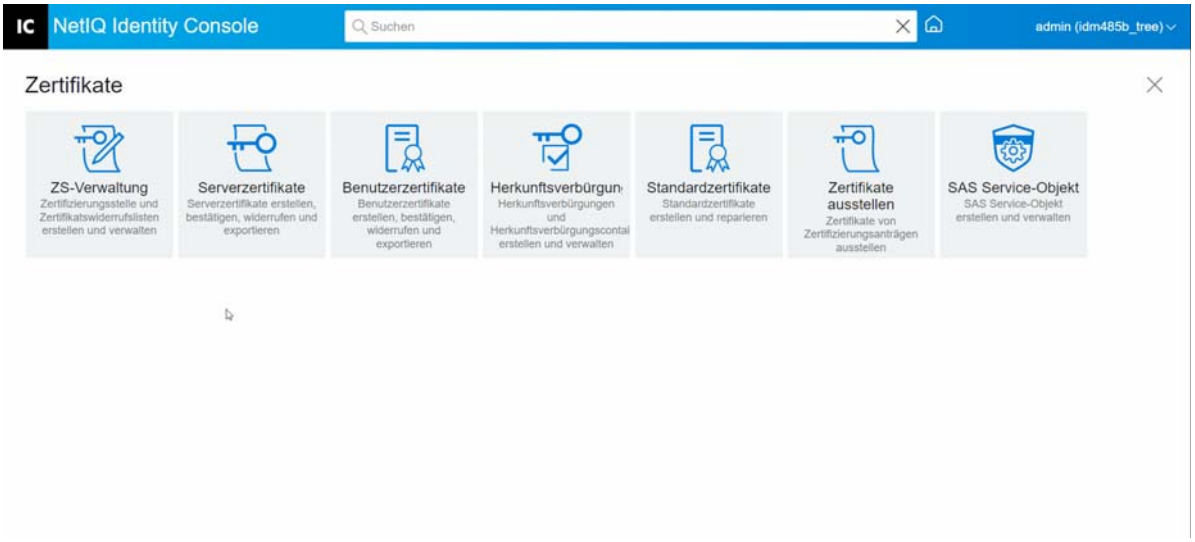
1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Serverzertifikate**.
2. Wählen Sie in der Dropdown-Liste den geeigneten Server aus.
3. Wählen Sie das geeignete Serverzertifikat aus der Liste aus und klicken Sie auf das Symbol ⊘.
4. Lesen Sie die Hinweise zum Risiko, das mit dem Widerruf von Serverzertifikaten verbunden ist, und klicken Sie auf **OK**.
5. Wählen Sie im nächsten Bildschirm einen gültigen Grund für den Widerruf aus der Dropdown-Liste aus, wählen Sie das Datum der Ungültigkeit aus und geben Sie beliebige weitere Kommentare an.
6. Klicken Sie auf **OK**, um das Widerrufen abzuschließen.

Serverzertifikatsobjekte löschen

Führen Sie die folgenden Schritte aus, um Serverzertifikatsobjekte zu entfernen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Serverzertifikate**.
2. Wählen Sie in der Dropdown-Liste den geeigneten Server aus.
3. Wählen Sie das geeignete Serverzertifikat aus der Liste aus und klicken Sie auf das Symbol 🗑.
4. Klicken Sie im nächsten Bildschirm auf **OK**.
5. Eine Meldung bestätigt die erfolgreiche Löschung des Serverzertifikatsobjekts.

Abbildung 17-2 *Serverzertifikate verwalten*



Benutzerzertifikate verwalten

Mit dem Benutzerzertifikatverwaltungsmodul können Sie die folgende Aufgabe ausführen:

Benutzerzertifikatsobjekte erstellen

Führen Sie die folgenden Schritte aus, um ein Benutzerzertifikatsobjekt zu erstellen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Benutzerzertifikate**.
2. Klicken Sie auf das Symbol +.
3. Geben Sie auf der Seite **Benutzerzertifikat erstellen** einen Namen in das Feld **Kurzname** ein, geben Sie einen Server an und wählen Sie eine der folgenden Optionen aus:
   - **Standard (Standardparameter):** Ermöglicht das Erstellen eines Standardbenutzerzertifikatsobjekts vom Typ RSA oder ECDSA.
   - **Benutzerdefiniert (Benutzer gibt Parameter an):** Ermöglicht die Angabe benutzerdefinierter Parameter für das Benutzerzertifikatsobjekt.
   - **Importieren:** Ermöglicht das Importieren einer Zertifikatsdatei im CERT- oder PKCS12-Format.
4. Klicken Sie nach der Angabe der Parameter auf **Weiter**, um die Zusammenfassung des Zertifikats zu überprüfen.
5. Klicken Sie im Bildschirm **Zusammenfassung** auf **OK**, um ein Benutzerzertifikatsobjekt zu erstellen.

Benutzerzertifikatsobjekte exportieren

Führen Sie die folgenden Schritte aus, um Benutzerzertifikatsobjekte zu exportieren:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Benutzerzertifikate**.
2. Wählen Sie in der Dropdown-Liste den geeigneten Server aus.
3. Wählen Sie das geeignete Benutzerzertifikat aus der Liste aus und klicken Sie auf das Symbol  .
4. Aktivieren Sie im nächsten Bildschirm das Kontrollkästchen **Privaten Schlüssel exportieren** und geben Sie ein Passwort zum Schutz des privaten Schlüssels an. Bestätigen Sie das Passwort und wählen Sie das Exportformat aus.

HINWEIS: Benutzerzertifikate können nur im PKCS12-Format exportiert werden.

5 Klicken Sie auf **OK**, um das Benutzerzertifikatsobjekt zu exportieren.

Benutzerzertifikatsobjekte bestätigen

Führen Sie die folgenden Schritte aus, um ein Benutzerzertifikatsobjekt zu bestätigen:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Benutzerzertifikate**.

2 Wählen Sie in der Dropdown-Liste den geeigneten Server aus.

3 Wählen Sie das geeignete Benutzerzertifikat aus der Liste aus und klicken Sie auf das Symbol  .

4 Eine Meldung bestätigt die erfolgreiche Bestätigung des Benutzerzertifikatsobjekts.

Benutzerzertifikatsobjekte widerrufen

Führen Sie die folgenden Schritte aus, um ein Benutzerzertifikatsobjekt zu widerrufen:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Benutzerzertifikate**.

2 Wählen Sie in der Dropdown-Liste den geeigneten Server aus.

3 Wählen Sie das geeignete Benutzerzertifikat aus der Liste aus und klicken Sie auf das Symbol  .

4 Lesen Sie die Hinweise zum Risiko, das mit dem Widerruf von Benutzerzertifikaten verbunden ist.

5 Wählen Sie aus der Dropdown-Liste einen gültigen Grund für den Widerruf aus, wählen Sie das Datum der Ungültigkeit aus und geben Sie beliebige weitere Kommentare an.

6 Klicken Sie auf **OK**, um das Widerrufen abzuschließen.

Benutzerzertifikatsobjekte löschen

Führen Sie die folgenden Schritte aus, um Benutzerzertifikatsobjekte zu entfernen:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Benutzerzertifikate**.

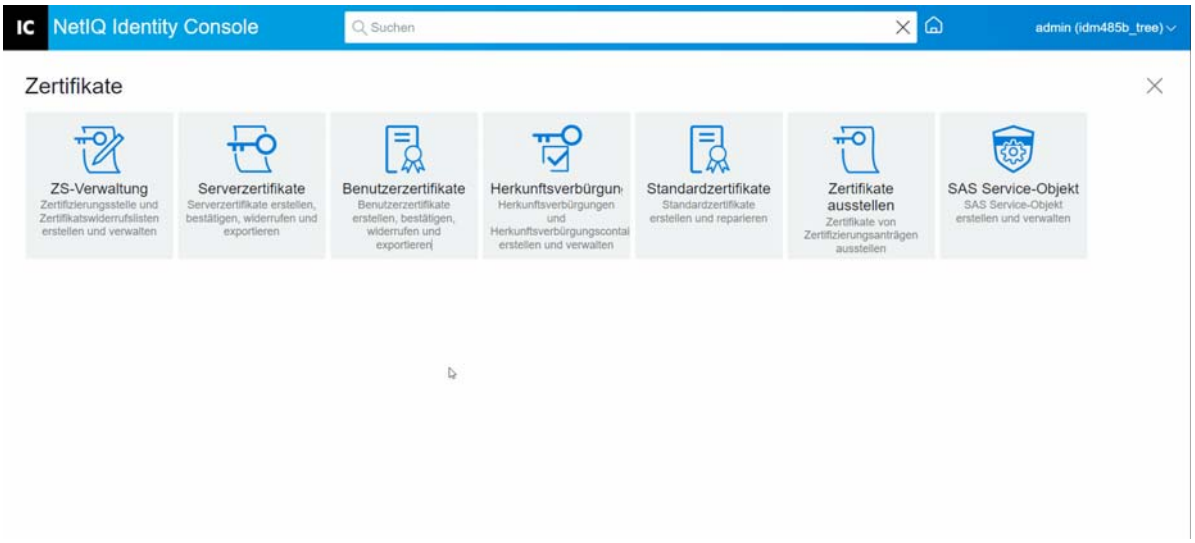
2 Wählen Sie in der Dropdown-Liste den geeigneten Server aus.

3 Wählen Sie das geeignete Benutzerzertifikat aus der Liste aus und klicken Sie auf das Symbol  .

4 Klicken Sie im nächsten Bildschirm auf **OK**.

5 Eine Meldung bestätigt die erfolgreiche Löschung des Benutzerzertifikatsobjekts.

Abbildung 17-3 *Benutzerzertifikate verwalten*



Herkunftsverbürgung und Container verwalten

Eine Herkunftsverbürgung stellt die Vertrauensgrundlage für das Public-Key-Verschlüsselungsverfahren dar. Herkunftsverbürgungen dienen der Bestätigung von Zertifikaten, die von anderen Zertifizierungsstellen signiert wurden. Herkunftsverbürgungen ermöglichen Sicherheit für SSL, sichere Email und zertifikatbasierte Authentifizierung.

Mit dem Herkunftsverbürgungsmodul können Sie die folgenden Aufgaben ausführen:

- „Herkunftsverbürgungscontainer erstellen“, auf Seite 100
- „Herkunftsverbürgungszertifikatsobjekt erstellen“, auf Seite 101
- „Herkunftsverbürgungszertifikatsobjekte exportieren“, auf Seite 101
- „Herkunftsverbürgungszertifikatobjekte bestätigen“, auf Seite 102
- „Herkunftsverbürgungszertifikatsobjekte löschen“, auf Seite 102
- „Herkunftsverbürgungscontainer löschen“, auf Seite 102

Herkunftsverbürgungscontainer erstellen

Führen Sie die folgenden Aufgaben aus, um einen Herkunftsverbürgungscontainer zu erstellen:

1. Klicken Sie auf der Identity Console-Landeseite auf **Zertifikate** > **Herkunftsverbürgungsverwaltung**. Das Kontrollkästchen **Herkunftsverbürgungscontainer** ist standardmäßig aktiviert.
2. Klicken Sie auf das Symbol +, um einen neuen Herkunftsverbürgungscontainer zu erstellen.
3. Geben Sie einen Namen für den Herkunftsverbürgungscontainer an.
4. Verwenden Sie die Objektauswahl, um nach dem entsprechenden Container zu suchen.
5. Klicken Sie auf die Schaltfläche **OK**.
6. Eine Meldung bestätigt die erfolgreiche Erstellung des Herkunftsverbürgungscontainers.

Herkunftsverbürgungszertifikatsobjekt erstellen

Führen Sie die folgenden Schritte aus, um ein Herkunftsverbürgungsobjekt zu erstellen:

1. Klicken Sie auf der Identity Console-Landeseite auf **Zertifikate** > **Herkunftsverbürgungsverwaltung**. Das Kontrollkästchen **Herkunftsverbürgungscontainer** ist standardmäßig aktiviert. Aktivieren Sie das Kontrollkästchen **Herkunftsverbürgung**.
2. Klicken Sie auf das Symbol +, um ein neues Herkunftsverbürgungsobjekt zu erstellen.
3. Geben Sie einen Namen für das Herkunftsverbürgungsobjekt an.
4. Wählen Sie in der Dropdown-Liste den entsprechenden Herkunftsverbürgungscontainer aus.
5. Wählen Sie durch Durchsuchen die entsprechende Zertifikatsdatei im Format `.der` oder `.b64` aus.

   HINWEIS: Jeder Zertifikattyp (Zertifizierungsstellenzertifikate, Zwischenzertifizierungsstellenzertifikate oder Benutzerzertifikate) kann in einem Herkunftsverbürgungsobjekt gespeichert werden.
6. Klicken Sie auf die Schaltfläche **OK**.
7. Eine Meldung bestätigt die erfolgreiche Erstellung des Herkunftsverbürgungsobjekts.

Herkunftsverbürgungszertifikatsobjekte exportieren

Führen Sie die folgenden Schritte aus, um Herkunftsverbürgungszertifikatsobjekte zu exportieren:

1. Klicken Sie auf der Identity Console-Landeseite auf **Zertifikate** > **Herkunftsverbürgungsverwaltung**. Das Kontrollkästchen **Herkunftsverbürgungscontainer** ist standardmäßig aktiviert. Aktivieren Sie das Kontrollkästchen **Herkunftsverbürgung**.
2. Wählen Sie das entsprechende Herkunftsverbürgungszertifikat aus der Liste aus und klicken Sie auf das Symbol .
3. Aktivieren Sie im nächsten Bildschirm das Kontrollkästchen **Privaten Schlüssel exportieren** und geben Sie ein Passwort zum Schutz des privaten Schlüssels an. Bestätigen Sie das Passwort und wählen Sie das Exportformat aus.

   HINWEIS: Herkunftsverbürgungszertifikate können nur im Format DER oder BASE64 exportiert werden.
4. Klicken Sie auf **OK**, um das Herkunftsverbürgungszertifikatsobjekt zu exportieren.

Herkunftsverbürgungszertifikatobjekte bestätigen

Führen Sie die folgenden Schritte aus, um Herkunftsverbürgungszertifikatsobjekte zu bestätigen:

1. Klicken Sie auf der Identity Console-Landeseite auf **Zertifikate** > **Herkunftsverbürgungsverwaltung**. Das Kontrollkästchen **Herkunftsverbürgungscontainer** ist standardmäßig aktiviert. Aktivieren Sie das Kontrollkästchen **Herkunftsverbürgung**.
2. Wählen Sie das entsprechende Herkunftsverbürgungszertifikat aus der Liste aus und klicken Sie auf das Symbol .
3. Eine Meldung bestätigt die erfolgreiche Bestätigung des Herkunftsverbürgungszertifikatsobjekts.

Herkunftsverbürgungszertifikatsobjekte löschen

Führen Sie die folgenden Schritte aus, um Herkunftsverbürgungszertifikatsobjekte zu entfernen:

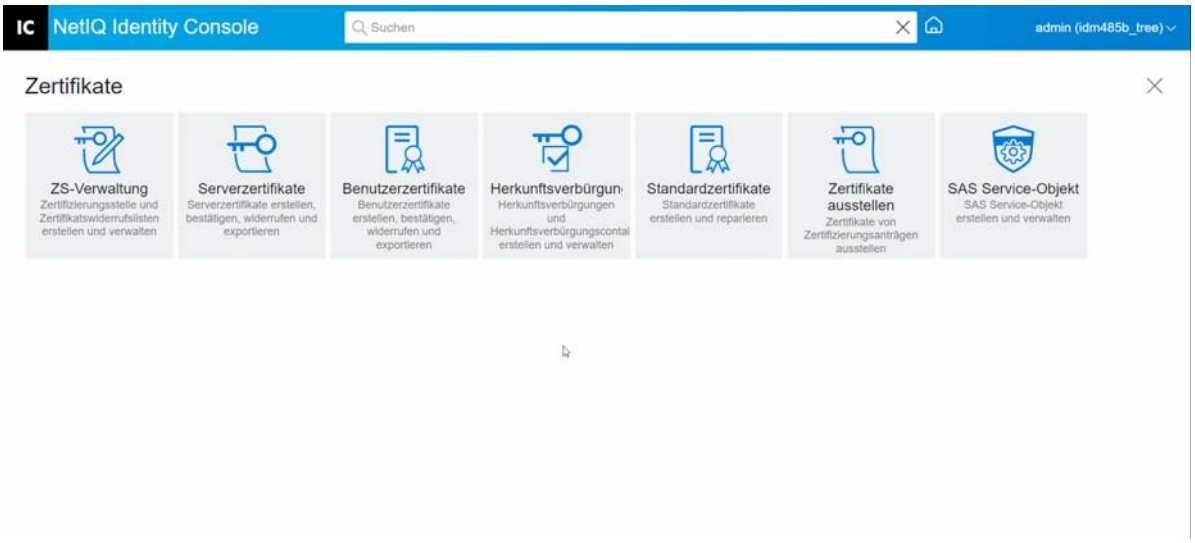
1. Klicken Sie auf der Identity Console-Landeseite auf **Zertifikate** > **Herkunftsverbürgungsverwaltung**. Das Kontrollkästchen **Herkunftsverbürgungscontainer** ist standardmäßig aktiviert. Aktivieren Sie das Kontrollkästchen **Herkunftsverbürgung**.
2. Wählen Sie das entsprechende Herkunftsverbürgungszertifikat aus der Liste aus und klicken Sie auf das Symbol .
3. Klicken Sie auf dem Warnbildschirm auf **OK**.
4. Eine Meldung bestätigt die erfolgreiche Entfernung des Herkunftsverbürgungszertifikatsobjekts.

Herkunftsverbürgungscontainer löschen

Führen Sie die folgenden Schritte aus, um einen Herkunftsverbürgungscontainer zu entfernen:

1. Klicken Sie auf der Identity Console-Landeseite auf **Zertifikate** > **Herkunftsverbürgungsverwaltung**. Das Kontrollkästchen **Herkunftsverbürgungscontainer** ist standardmäßig aktiviert.
2. Wählen Sie den entsprechenden Herkunftsverbürgungscontainer aus der Liste aus und klicken Sie auf das Symbol .
3. Klicken Sie auf dem Warnbildschirm auf **OK**.
4. Eine Meldung bestätigt die erfolgreiche Entfernung des Herkunftsverbürgungscontainers.

Abbildung 17-4 *Herkunftsverbürgungscontainer verwalten*



Standardserverzertifikatsobjekte erstellen

Bei der Installation von Certificate Server werden Standardserverzertifikatsobjekte erstellt.

- SSL CertificateDNS - *Servername*
- Ein Zertifikat für jede auf dem Server konfigurierte IP-Adresse (IPAG*xxx.xxx.xxx.xxx* - *Servername*)
- Ein Zertifikat für jeden auf dem Server konfigurierten DNS-Namen (DNSAG*www.beispiel.com* - *Servername*)

HINWEIS: eDirectory erstellt das Zertifikat „SSL CertificateIP“ nicht automatisch. „SSL CertificateDNS“ enthält alle IP-Adressen, die im alternativen Antragstellernamen aufgelistet sind. Wenn Sie versuchen, die Standardzertifikate mit Identity Console zu erstellen oder zu reparieren, wird das Zertifikat „SSL CertificateIP“ standardmäßig nicht erstellt oder repariert. Die Plugin-Benutzeroberfläche stellt jedoch ein Kontrollkästchen bereit, das Sie aktivieren können, um das Standardverhalten außer Kraft zu setzen und die Erstellung/Reparatur des Zertifikats „SSL CertificateIP“ zu erzwingen.

eDirectory 9.0 und höher erstellt automatisch ECDSA-Zertifikate, wenn die Organisationszertifizierungsstelle über ein ECDSA-Zertifikat verfügt.

Wenn diese Zertifikate aus einem beliebigen Grund beschädigt werden oder ungültig geworden sind oder sie einfach die vorhandenen Standardzertifikate ersetzen möchten, können Sie den Assistenten „Create Default Server Certificates“ (Standardserverzertifikate erstellen) wie im folgenden Verfahren beschrieben verwenden:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Standardzertifikate**.
2. Wählen Sie den oder die Server aus, für den bzw. für die Sie Standardzertifikate erstellen möchten, und klicken Sie dann auf **Weiter**.

3 Wählen Sie „Ja“ aus, wenn Sie die vorhandenen Standardserverzertifikate überschreiben möchten, oder „Nein“, wenn Sie die vorhandenen Standardserverzertifikate nur dann überschreiben möchten, wenn sie ungültig sind.

4 (Nur Einzelserver) Wenn Sie die vorhandene DNS-Adresse verwenden möchten, wählen Sie diese Option aus. Wenn Sie eine andere DNS-Adresse verwenden möchten, wählen Sie diese Option aus und geben Sie die neue DNS-Adresse an.

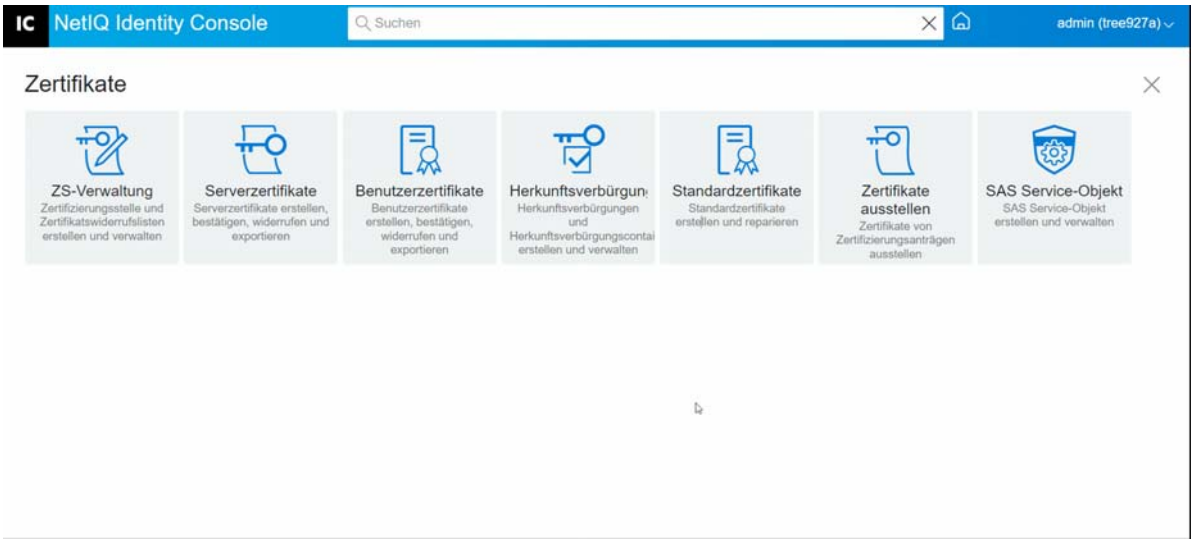
5 (Nur Einzelserver) Wenn Sie die vorhandene Standard-IP-Adresse verwenden möchten, wählen Sie diese Option aus. Wenn Sie eine andere IP-Adresse verwenden möchten, wählen Sie diese Option aus und geben Sie die neue IP-Adresse an.

6 Klicken Sie auf **Weiter**.

7 Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertigstellen**.

Wenn Sie mehr Kontrolle über die Erstellung des Serverzertifikatsobjekts haben möchten, können Sie das Serverzertifikatsobjekt auch manuell erstellen. Weitere Informationen finden Sie im „Serverzertifikatsobjekte erstellen“, auf Seite 95.

Abbildung 17-5 *Standardserverzertifikatsobjekte erstellen*



Zertifikate mit öffentlichem Schlüssel ausstellen

Ihre Organisationszertifizierungsstelle funktioniert auf die gleiche Weise wie eine externe Zertifizierungsstelle. Das bedeutet, dass sie Zertifikate aus Zertifizierungsanträgen ausstellen kann. Sie können Zertifikate mithilfe der Organisationszertifizierungsstelle ausstellen, wenn ein Benutzer einen Zertifizierungsantrag zum Signieren sendet. Der Benutzer, der das Zertifikat beantragt, kann dann das ausgestellte Zertifikat direkt in die verschlüsselungsfähige Anwendung importieren.

Mit dieser Aufgabe können Sie Zertifikate für verschlüsselungsfähige Anwendungen generieren, die keine Serverzertifikatsobjekte anerkennen.

Führen Sie die folgenden Schritte aus, um ein Zertifikat auszustellen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **Zertifikat ausstellen**.
2. Wählen Sie durch Durchsuchen eine CSR-Datei aus.
3. Wählen Sie den entsprechenden Schlüsseltyp und die entsprechende Schlüsselverwendung unter „Schlüsselverwendungsangaben“ aus. Mit diesen Optionen können Sie einen Schlüsseltyp auswählen. Mit jedem Schlüsseltyp ist eine vordefinierte Schlüsselnutzung verbunden:
   - 3a **Nicht angegeben:** Diese Option ist standardmäßig aktiviert und aktiviert keine Schlüsselverwendung im Zertifikat.
   - 3b **Zertifizierungsstelle:** Mit dieser Option werden die Schlüsselverwendungen „Zertifikatsignatur“ und „CRL-Signatur“ aktiviert.
   - 3c **Verschlüsselung:** (Verschlüsselung) Diese Option aktiviert die Schlüsselsyntax "Key Encipherment" (Schlüsselverschlüsselung).
   - 3d **Signatur:** (Signatur) Diese Option aktiviert die Schlüsselsyntax "Digital Signature" (Digitalsignatur).
   - 3e **SSL oder TSL:** (SSL oder TLS) Diese Option konfiguriert den Schlüssel, sodass er in SSL- oder TLS-Transaktionen verwendet werden kann.
   - 3f **Benutzerdefiniert:** Mit dieser Option können Sie eine beliebige oder auch alle Schlüsselverwendungsoptionen manuell auswählen.
   - 3g **Die Schlüsselnutzungserweiterung als "Kritisch" markieren:** Sie können die Nutzungserweiterung jedes Schlüsseltyps außer "Nicht angegeben" als "Kritisch" kennzeichnen. Jede kritische Erweiterung muss von der empfangenden Software korrekt interpretiert werden, damit das Zertifikat überhaupt verwendet werden kann. Die Markierung einer Erweiterung als kritisch stellt daher ein gewisses Risiko dar, da nicht alle Anwendungen das Zertifikat nutzen können. Bei allgemein bekannten Erweiterungen wie etwa der Schlüsselnutzung ist das Risiko jedoch gering. Wenn eine Schlüsselnutzung angegeben wird, sollte die Erweiterung in der Regel als kritisch markiert werden.
4. Sie können im Zertifikat eine Erweiterung für die **Verwendung erweiterter Schlüssel** kodieren lassen. Um diese Funktion zu aktivieren, wählen Sie **Verwendung erweiterter Schlüssel aktivieren** aus:
   - 4a **Server:** Diese Option aktiviert die Verwendung erweiterter Schlüssel bei der Serverauthentifizierung.
   - 4b **Benutzer:** Diese Option aktiviert die Verwendung erweiterter Schlüssel bei der Benutzerauthentifizierung und für den Email-Schutz.
   - 4c **Benutzerdefiniert:** Mit dieser Option können Sie beliebige oder alle Verwendungen erweiterter Schlüssel auswählen.
   - 4d **Beliebig:** Ermöglicht die Verwendung des Schlüssels für jede beliebige erweiterte Schlüsselnutzung.
   - 4e **Erweiterung für Verwendung erweiterter Schlüssel auf 'kritisch' festlegen:** Jede kritische Erweiterung muss von der empfangenden Software korrekt interpretiert werden, damit das Zertifikat überhaupt verwendet werden kann. Die Markierung einer Erweiterung als kritisch stellt daher ein gewisses Risiko dar, da nicht alle Anwendungen das Zertifikat nutzen können. Da viele Anwendungen die erweiterte Schlüsselnutzung nicht kennen,

stellt die Markierung dieser Erweiterung als kritisch ein erhebliches Risiko für die Annahme des Zertifikats durch eine bestimmte Anwendung dar. Die Erweiterung sollte deshalb nur als kritisch markiert werden, wenn es unbedingt nötig ist.

5 Wählen Sie die geeigneten Einstellungen unter **Grundlegende Einschränkungen** aus:

5a Zertifikatstyp:

5a1 Nicht angegeben: Wählen Sie diese Option, wenn Sie dem Zertifikat keine grundlegende Beschränkung hinzufügen möchten.

5a2 Zertifizierungsstelle: Wählen Sie diese Option, wenn Sie dem Zertifikat die Einstellung "Zertifizierungsstelle" als Erweiterung für eine grundlegende Beschränkung hinzufügen möchten. Wenn das Zertifikat für eine Zertifizierungsstelle bestimmt ist, muss diese Option ausgewählt werden.

5a3 Endentität: Wählen Sie diese Option, wenn Sie dem Zertifikat eine Erweiterung für eine grundlegende Beschränkung hinzufügen möchten, die angibt, das es sich um eine Endentität (d.h. keine Zertifizierungsstelle) handelt. Hinweis: Wenn ein Zertifikat vom Typ Endentität ist, sollte die Pfadlänge auf "Nicht angegeben" gesetzt werden.

5b Pfadlänge:

5b1 Nicht angegeben: Wählen Sie diese Option, wenn Sie nicht festlegen möchten, wie viele Ebenen untergeordneter Zertifizierungsstellen unter dieser Zertifizierungsstelle angelegt werden dürfen.

HINWEIS: Wenn ein Zertifikat vom Typ Endentität ist, sollte die Pfadlänge auf "Nicht angegeben" gesetzt werden.

5b2 Spezifisch: Wählen Sie diese Option, wenn Sie festlegen möchten, wie viele Ebenen untergeordneter Zertifizierungsstellen unter dieser Zertifizierungsstelle angelegt werden dürfen. Klicken Sie auf die Pfeilschaltflächen, um die Pfadlänge einzustellen.

HINWEIS: Wenn eine Zertifikat für eine untergeordnete Zertifizierungsstelle erstellt wird, muss die Pfadlänge konsistent mit der der übergeordneten Zertifizierungsstelle sein. Beispiel: Wenn die übergeordnete Zertifizierungsstelle eine Pfadlänge von 3 hat, muss die Pfadlänge der untergeordneten Zertifizierungsstelle 2 oder weniger sein. Wenn für die übergeordnete Zertifizierungsstelle keine Pfadlänge angegeben wurde, kann die untergeordnete Zertifizierungsstelle entweder ebenfalls keine Angabe haben oder eine beliebige spezifische Pfadlänge.

5c Grundlegende Beschränkungserweiterung auf kritisch setzen: Allgemein muss die grundlegende Beschränkungserweiterung bei Zertifikaten für Zertifizierungsstellen auf kritisch gesetzt werden. Jede kritische Erweiterung muss von der empfangenden Software korrekt interpretiert werden, damit das Zertifikat überhaupt verwendet werden kann. Die Markierung einer Erweiterung als kritisch stellt daher ein gewisses Risiko dar, da nicht alle Anwendungen das Zertifikat nutzen können. Bei allgemein bekannten Erweiterungen wie etwa der grundlegenden Beschränkung ist das Risiko jedoch gering.

6 Legen Sie die folgenden Zertifikatparameter fest:

6a Subjektname: Enthält den vollständigen Namen Ihres eDirectory-Baums.

6b Subjektname: Enthält den vollständigen Namen Ihres eDirectory-Baums.

6c **Gültigkeitsdauer:** Verwenden Sie die Dropdown-Liste, um den Zeitraum anzugeben, in dem das Zertifikat gültig ist. Die möglichen Einstellungen reichen von 6 Monaten bis zum Jahr 2036 (eine Zeitbeschränkung, die auf einer 32-Bit-Zeitangabe basiert). Wenn Sie die Option "Datumsangaben einfügen" wählen, können Sie in die Felder "Gültigkeitsdatum" und "Ablaufdatum" Anfang und Ende eines benutzerdefinierten Gültigkeitszeitraums eingeben. Das Ablaufdatum muss innerhalb des Gültigkeitszeitraums der Zertifizierungsstelle liegen.

6c1 **Gültigkeitsdatum:** Ermöglicht die Anzeige oder Änderung des Datums und der Uhrzeit des Anfangs der Gültigkeit des Zertifikats.

6c2 **Ablaufdatum:** Ermöglicht die Anzeige oder Änderung des Datums und der Uhrzeit des Endes der Gültigkeit des Zertifikats.

6d **Benutzerdefinierte Erweiterungen:** Diese Funktion ermöglicht Certificate Server die Unterstützung beliebiger Standard- oder benutzerdefinierter Erweiterungen, die Sie beim Erstellen eines Zertifikats einbeziehen möchten. Erweiterungen müssen zuvor erstellt und in einer Datei (eine Erweiterung je Datei) gespeichert worden sein. Jede Erweiterung muss nach ASN.1 gemäß Definition in IETF RFC 2459/3280 Abschnitt 4.2 verschlüsselt sein.

Wenn Sie beim Erstellen eines Zertifikats benutzerdefinierte Erweiterungen einbeziehen möchten, klicken Sie auf "Neu", wählen Sie die Datei aus, in der die benutzerdefinierte Erweiterung enthalten ist, und fügen Sie diese dem Zertifikat hinzu. Wiederholen Sie diesen Vorgang, wenn Sie weitere Erweiterungen hinzufügen möchten.

Um eine Datei mit einer benutzerdefinierten Erweiterung zu löschen, wählen Sie sie aus und klicken Sie auf das Symbol  .

7 Wählen Sie das geeignete Zertifikatformat aus den folgenden Optionen aus:

7a **Datei im binären DER-Format:** Mit dieser Option können Sie ein Zertifikat in eine Datei, die im Feld „Dateiname“ angezeigt wird, speichern oder exportieren. Die Zertifikatdatei wird standardmäßig mit der Erweiterung **.**DER versehen und im Stammverzeichnis des Laufwerks C: einer Windows-basierten Identity Console-Arbeitsstation und im Basisverzeichnis einer Linux-basierten Identity Console-Arbeitsstation gespeichert.

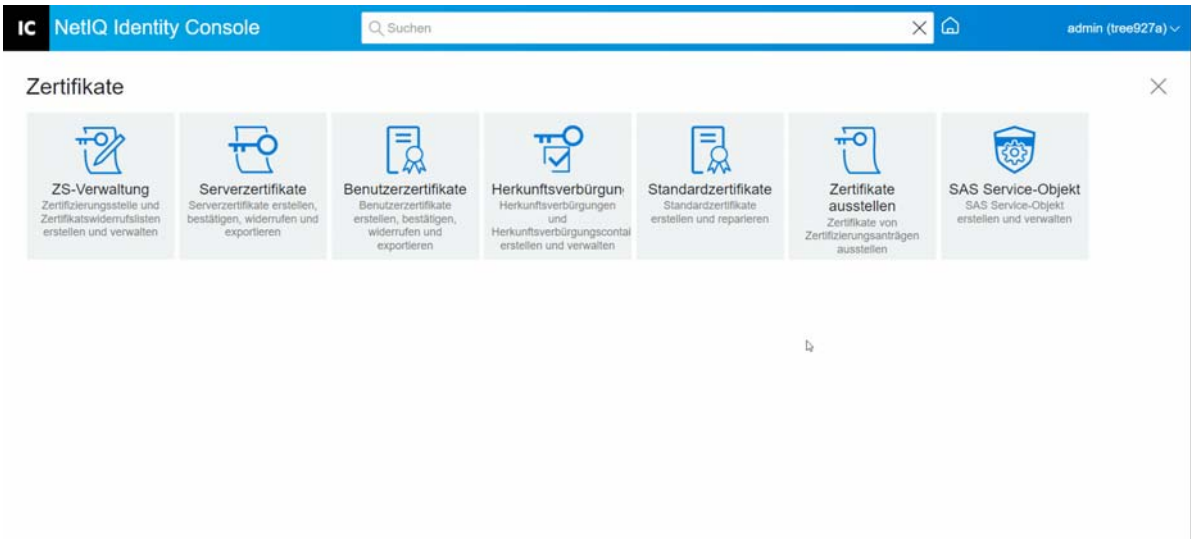
7b **Datei im Base64-Format:** Mit dieser Option können Sie entweder einen Zertifizierungsantrag in einer Datei speichern, die im Feld „Dateiname“ angegeben wird, oder ein Zertifikat in diese Datei exportieren. Die Zertifikat- und Zertifizierungsantragsdateien werden standardmäßig mit der Erweiterung „.B64“ versehen und im Stammverzeichnis des Laufwerks C: einer Windows-basierten Identity Console-Arbeitsstation und im Basisverzeichnis eines Linux-basierten Identity Console-Arbeitsstation gespeichert.

7c **Datei im CER-Format:** Mit dieser Option können Sie entweder einen Zertifizierungsantrag in einer Datei speichern, die im Feld „Dateiname“ angegeben wird, oder ein Zertifikat in diese Datei exportieren. Die Zertifikat- und Zertifizierungsantragsdateien werden standardmäßig mit der Erweiterung „.CER“ versehen und im Stammverzeichnis des Laufwerks C: einer Windows-basierten Identity Console-Arbeitsstation und im Basisverzeichnis eines Linux-basierten Identity Console-Arbeitsstation gespeichert.

8 Überprüfen Sie die Zusammenfassung des Zertifikats im nächsten Bildschirm, und klicken Sie auf **OK**.

9 Eine Meldung bestätigt die erfolgreiche Ausstellung des Zertifikats.

Abbildung 17-6 *Zertifikate mit öffentlichem Schlüssel ausstellen*



SAS Service-Objekt verwalten

Das SAS Service-Objekt ermöglicht die Kommunikation zwischen einem Server und dessen Serverzertifikaten. Wenn Sie einen Server aus einem eDirectory-Baum entfernen, müssen Sie auch das mit diesem Server verknüpfte SAS Service-Objekt löschen. Gleichermaßen müssen Sie das SAS Service-Objekt für diesen Server wieder erstellen, wenn Sie den Server erneut in den Baum aufnehmen. Andernfalls können Sie keine neuen Serverzertifikate erstellen.

Das SAS Service-Objekt wird automatisch als Teil der Serverzustandsprüfung erstellt. Sie sollten es nicht manuell erstellen müssen.

Sie können nur dann ein neues SAS Service-Objekt erstellen, wenn sich im selben Container wie das Objekt noch kein entsprechend benanntes SAS Service-Objekt befindet. Für einen Server namens WAKE benötigen Sie beispielsweise ein SAS Service-Objekt namens „SAS Service - WAKE“. Das Dienstprogramm fügt dem SAS-Objekt die DS-Zeiger aus dem Serverobjekt und dem Serverobjekt die DS-Zeiger aus dem SAS-Objekt hinzu. Außerdem richtet es die entsprechenden Zugriffssteuerungslisteneinträge für das SAS Service-Objekt ein.

Wenn bereits ein SAS Service-Objektmit dem entsprechenden Namen vorhanden ist, können Sie kein neues SAS Service-Objekt erstellen. Es kann jedoch sein, dass die DS-Zeiger des alten SAS Service-Objekts falsch sind oder fehlen oder dass die Zugriffssteuerungslisten nicht korrekt sind. In diesem Fall können Sie das fehlerhafte SAS Service-Objekt löschen und im Identity Console-Portal ein neues erstellen.

SAS Service-Objekte erstellen oder löschen

Führen Sie die folgenden Schritte aus, um ein SAS Service-Objekt zu erstellen oder zu löschen:

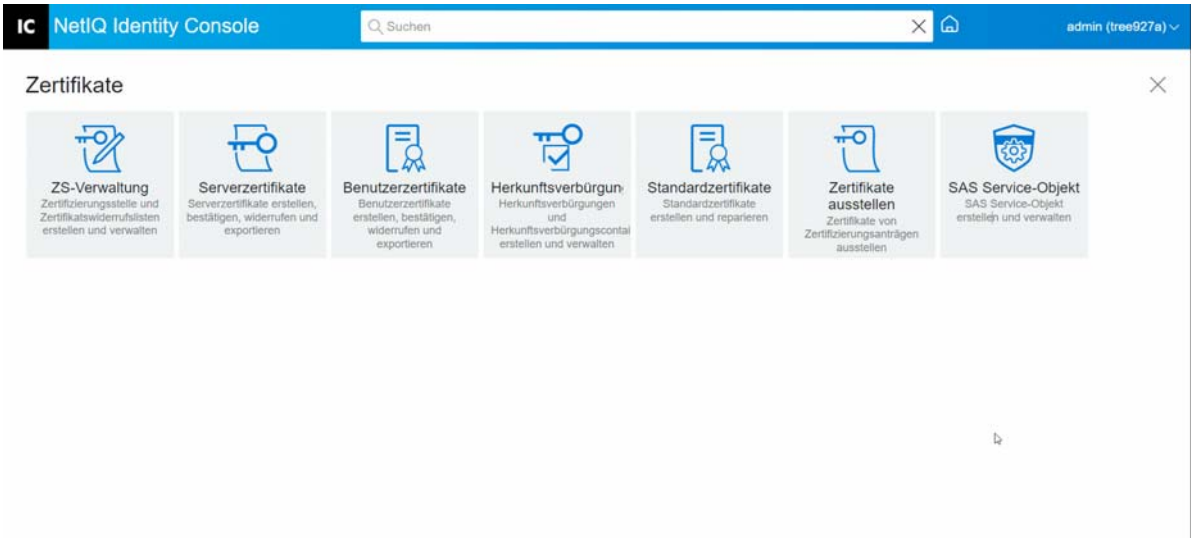
1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Zertifikate** > **SAS Service-Objekt**.
2. Wenn kein SAS Service-Objekt für einen vorhandenen Server erstellt wurde, klicken Sie auf das Symbol +, um ein neues zu erstellen.

3 Eine Meldung bestätigt die erfolgreiche Erstellung des SAS Service-Objekts.

4 Um ein SAS Service-Objekt zu entfernen, klicken Sie auf das Symbol .

5 Klicken Sie im Bestätigungsbildschirm auf **OK**, um ein SAS Service-Objekt zu entfernen.

Abbildung 17-7 *SAS Service-Objekte verwalten*



18 Authentifizierungs-Framework verwalten

Mit dem Authentifizierungsmodul können Sie die folgenden Aufgaben ausführen:

- „Anmeldemethoden und Anmeldefolgemethoden und zugehörige Sequenzen verwalten“, auf Seite 111
- „Verwalten von Passwortrichtlinien“, auf Seite 117
- „Sicherheitsabfragensätze verwalten“, auf Seite 123

Anmeldemethoden und Anmeldefolgemethoden und zugehörige Sequenzen verwalten

NMAS unterstützt eine Reihe von Anmeldemethoden und Anmeldefolgemethoden von NetIQ und von Drittanbieter-Authentifizierungsentwicklern. Bestimmte Methoden erfordern zusätzliche Hardware und Software. Stellen Sie sicher, dass Sie über die erforderliche Hardware und Software für die Methoden verfügen, die Sie verwenden möchten.

Dieser Abschnitt beschreibt die Installation, Einrichtung und Konfiguration von Anmeldemethoden, Anmeldefolgemethoden und Sequenzen für NMAS.

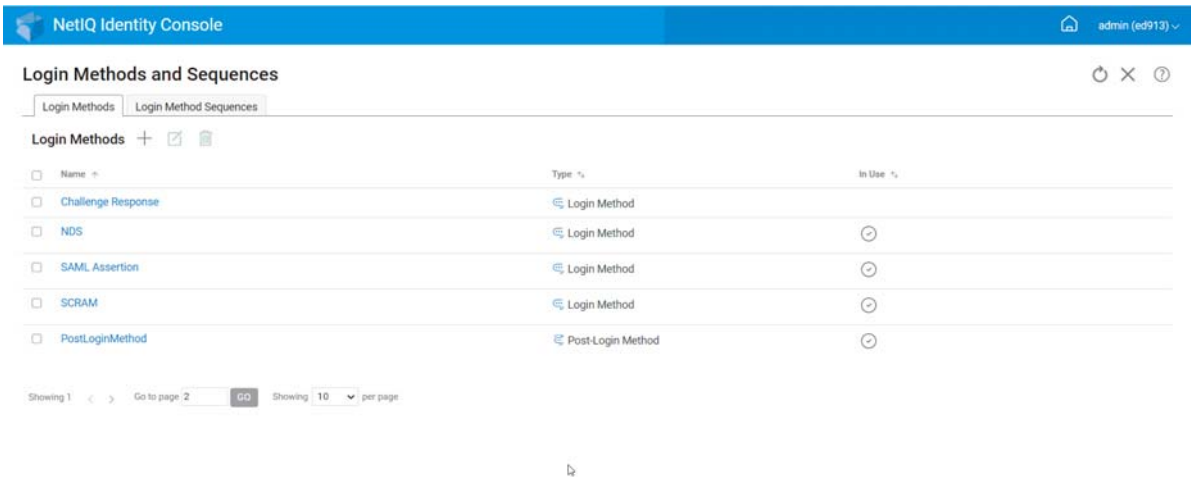
- „Anmeldemethode oder Anmeldefolgemethode installieren“, auf Seite 111
- „Vorhandene Anmeldemethode oder Anmeldefolgemethode aktualisieren“, auf Seite 112
- „Anmeldemethoden oder Anmeldefolgemethoden deinstallieren“, auf Seite 113
- „Neue Anmeldesequenzen erstellen“, auf Seite 114
- „Anmeldemethodensequenzen ändern“, auf Seite 114
- „Anmeldemethodensequenzen autorisieren oder Autorisierungen für Anmeldemethodensequenzen aufheben“, auf Seite 115
- „Standard-Anmeldemethodensequenzen festlegen“, auf Seite 116
- „Anmeldemethodensequenzen löschen“, auf Seite 117

Anmeldemethode oder Anmeldefolgemethode installieren

Um eine Anmeldemethode zu installieren, führen Sie die folgenden Aufgaben aus:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.
2. Klicken Sie auf das Symbol +, um eine neue Anmeldemethode zu installieren.
3. Wählen Sie durch Durchsuchen die Anmeldemethodendatei (.zip) aus, die Sie installieren möchten, und klicken Sie dann auf **Weiter**.
4. Befolgen Sie die Anweisungen im Installationsassistenten, um den Vorgang zum Installieren der Anmeldemethode abzuschließen.

Abbildung 18-1 *Neue Anmeldemethode installieren*

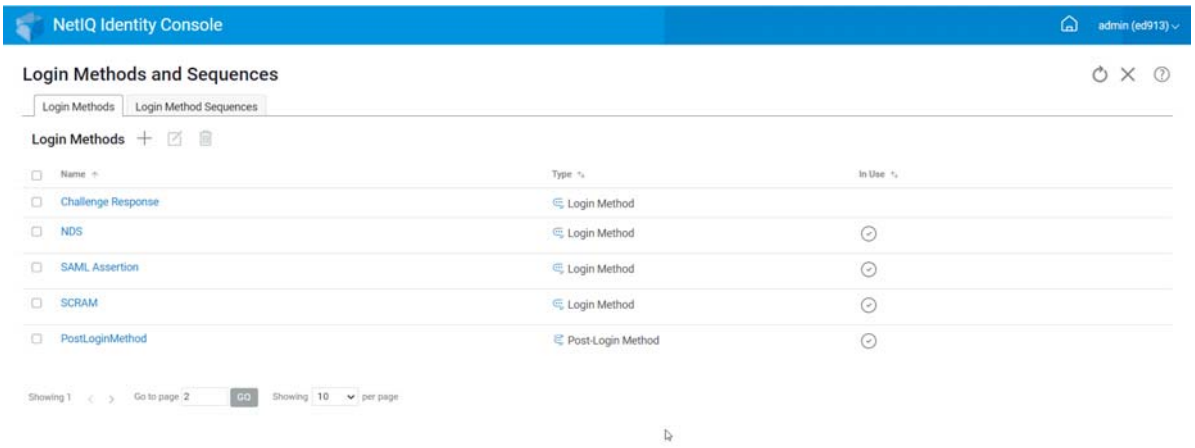


Vorhandene Anmeldemethode oder Anmeldefolgemethode aktualisieren

Führen Sie die folgenden Schritte aus, um eine vorhandene Anmeldemethode zu aktualisieren:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.
2. Wählen Sie aus der Liste die Anmeldemethode aus, die Sie aktualisieren möchten, und klicken Sie auf das Symbol ☑.
3. Wählen Sie durch Durchsuchen die Anmeldemethodendatei (.zip) aus, die Sie aktualisieren möchten, und klicken Sie dann auf **Weiter**.
4. Befolgen Sie die Anweisungen im Aktualisierungsassistenten, um die Aktualisierung der Anmeldemethode abzuschließen.

Abbildung 18-2 *Vorhandene Anmeldemethoden aktualisieren*

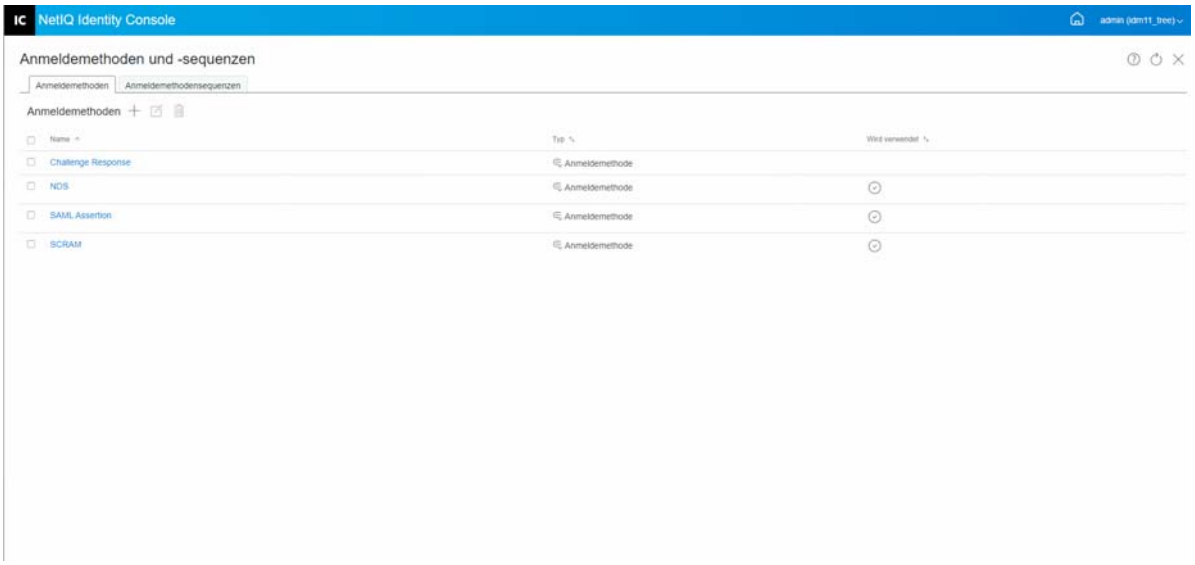


Anmeldemethoden oder Anmeldefolgemethoden deinstallieren

Führen Sie die folgenden Schritte aus, um eine Anmeldemethode oder eine Anmeldefolgemethode zu deinstallieren:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.
2. Wählen Sie in der Liste die Anmeldemethode(n) aus, die Sie deinstallieren möchten, und klicken Sie auf das Symbol .
3. Klicken Sie im nächsten Bildschirm auf **OK**.
4. Eine Meldung bestätigt die erfolgreiche Deinstallation der Anmeldemethode(n).

Abbildung 18-3 *Anmeldemethode deinstallieren*



Neue Anmeldesequenzen erstellen

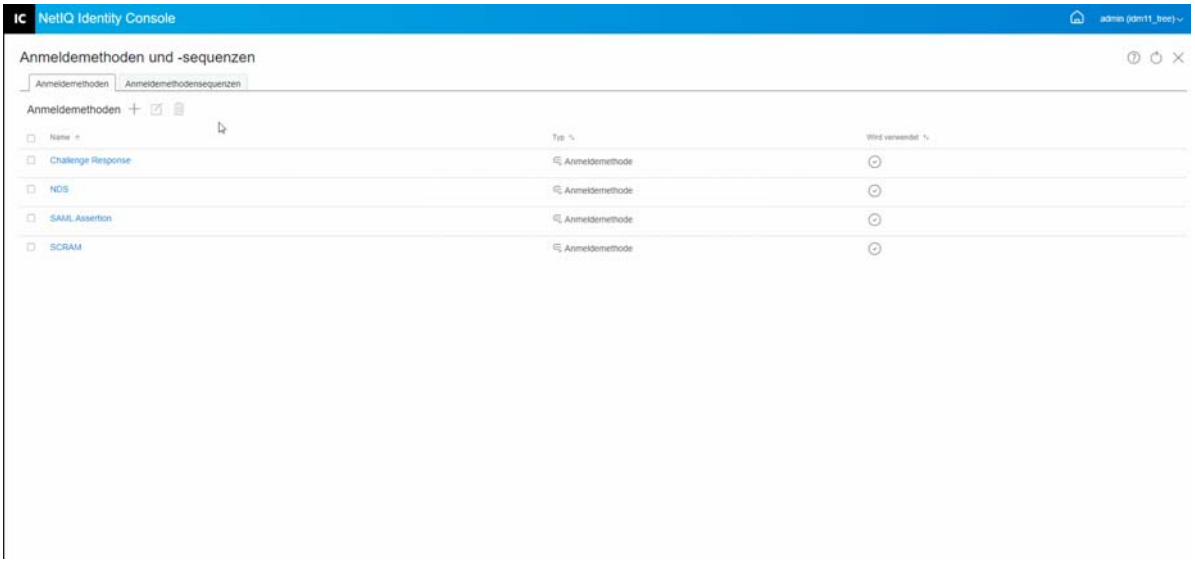
Nachdem Sie verschiedene Anmeldemethoden für Ihre Umgebung erstellt haben, können Sie festlegen, in welcher Reihenfolge diese Methoden verwendet werden sollen. Führen Sie die folgenden Schritte aus, um eine neue Anmeldemethodensequenz zu erstellen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.
2. Wählen Sie die Registerkarte **Anmeldemethodensequenzen** aus.
3. Klicken Sie auf das Symbol +, um eine neue Anmeldemethodensequenz zu erstellen.
4. Geben Sie im Feld **Name** den gewünschten Namen an und treffen Sie unter **Sequenztyp** die gewünschte Wahl.
5. Wählen Sie die erforderlichen Anmeldemethoden und Anmeldefolgemethoden aus der Liste der verfügbaren Anmeldemethoden und Anmeldefolgemethoden aus.

   HINWEIS: Sie können die Reihenfolge der Anmeldemethoden durch Klicken auf die Auf- und Abwärtspfeile der Anmeldemethode ändern.

   ---
6. Klicken Sie auf die Schaltfläche **Erstellen**.
7. Eine Meldung bestätigt die erfolgreiche Erstellung der neuen Anmeldemethodensequenz.

Abbildung 18-4 *Anmeldemethodensequenz erstellen*



Anmeldemethodensequenzen ändern

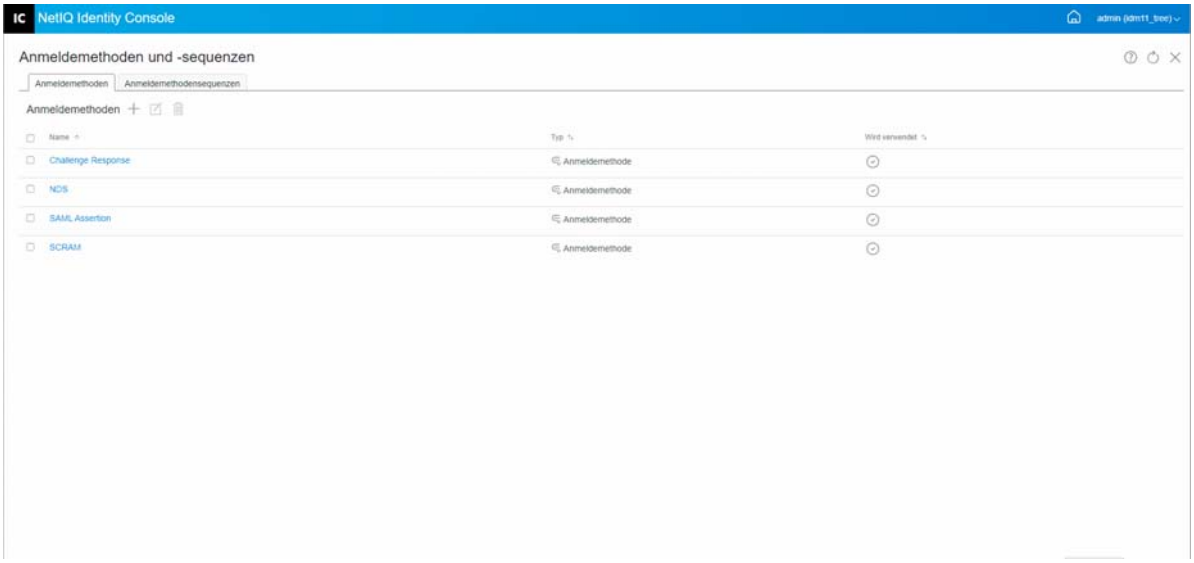
Führen Sie die folgenden Schritte aus, um eine vorhandene Anmeldemethodensequenz zu ändern:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.
2. Wählen Sie die Registerkarte **Anmeldemethodensequenzen** aus.
3. Klicken Sie auf das Symbol, um eine vorhandene Anmeldemethodensequenz zu ändern.

4 Nehmen Sie die erforderlichen Änderungen auf der Seite **Anmeldemethodensequenz ändern** vor und klicken Sie auf **Speichern**.

5 Eine Meldung bestätigt die erfolgreiche Änderung der neuen Anmeldemethodensequenz.

Abbildung 18-5 *Anmeldemethodensequenzen ändern*



Anmeldemethodensequenzen autorisieren oder Autorisierungen für Anmeldemethodensequenzen aufheben

Eine Anmeldemethodensequenz sollte autorisiert und als Standard festgelegt werden, um sie mit Benutzern, Containern und Partitionen zu verknüpfen. Führen Sie die folgenden Schritte aus, um eine Anmeldemethodensequenz zu autorisieren:

1 Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.

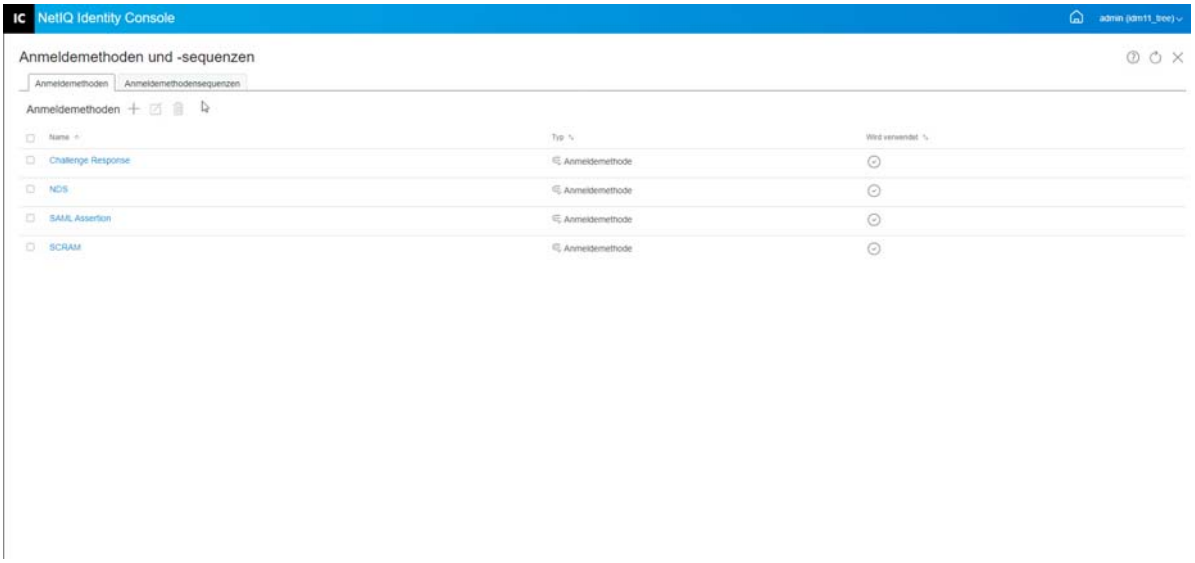
2 Wählen Sie die Registerkarte **Anmeldemethodensequenzen** aus.

3 Wählen Sie die entsprechende Anmeldemethodensequenz aus der Liste aus und klicken Sie auf das Symbol ⓥ.

4 Um die Autorisierung einer Anmeldemethodensequenz aufzuheben, wählen Sie die Anmeldemethodensequenz aus und klicken Sie auf das Symbol ⓧ.

5 Alternativ können Sie Anmeldemethodensequenzen auch über das Dropdown-Menü unter der Spalte **Autorisiert** in der Liste der Anmeldemethodensequenzen autorisieren bzw. die Autorisierung aufheben.

Abbildung 18-6 *Anmeldemethodensequenzen autorisieren oder Autorisierungen für Anmeldemethodensequenzen aufheben*

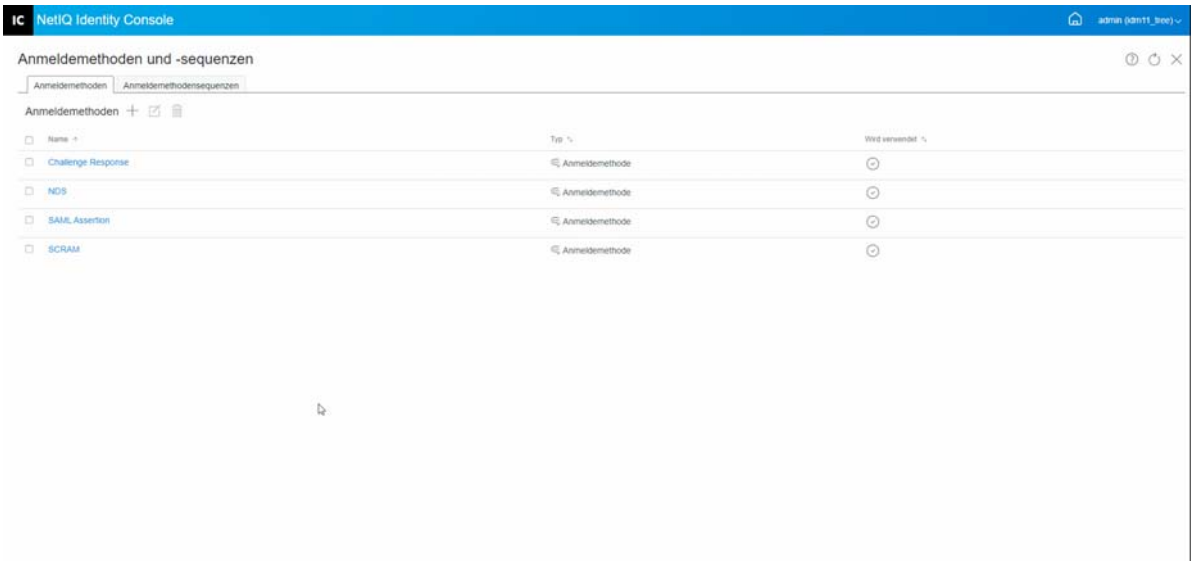


Standard-Anmeldemethodensequenzen festlegen

So legen Sie eine Standardanmeldesequenz fest, damit die Benutzer bei der Anmeldung keine Anmeldesequenz angeben müssen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.
2. Wählen Sie die Registerkarte **Anmeldemethodensequenzen** aus.
3. Aktivieren Sie das Symbol , um eine autorisierte Anmeldemethodensequenz als Standard festzulegen.

Abbildung 18-7 *Standard-Anmeldemethodensequenzen festlegen*

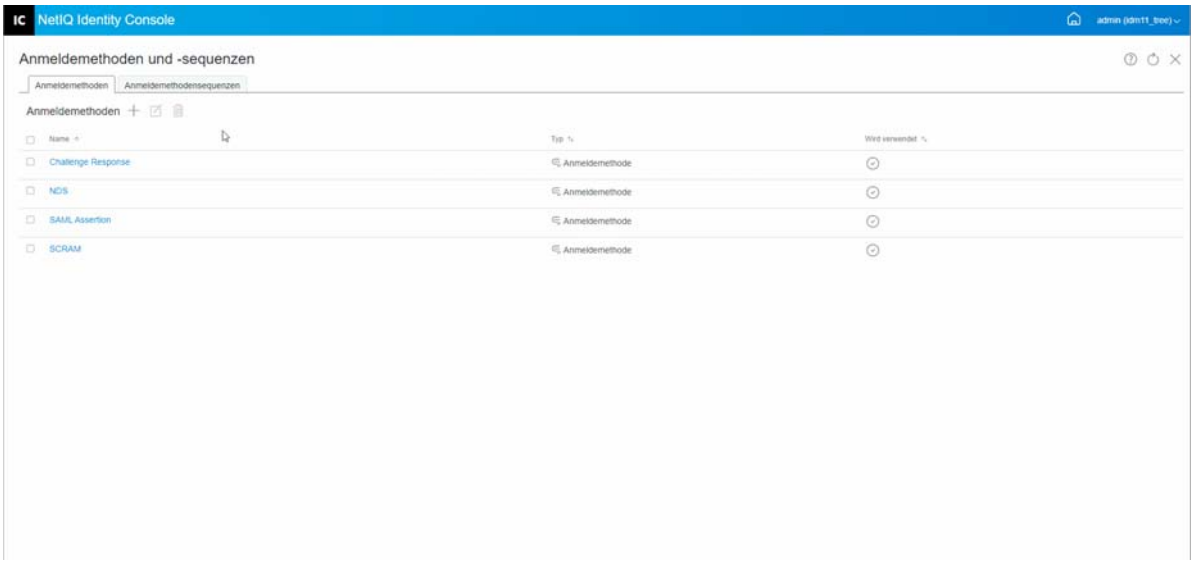


Anmeldemethodensequenzen löschen

So löschen Sie eine Anmeldemethodensequenz:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Anmeldemethoden und -sequenzen**.
2. Wählen Sie die Registerkarte **Anmeldemethodensequenzen** aus.
3. Wählen Sie die entsprechende Anmeldemethodensequenz aus der Liste aus und klicken Sie auf das Symbol .
4. Klicken Sie im nächsten Bestätigungsbildschirm auf **OK**.

Abbildung 18-8 *Anmeldemethodensequenz löschen*



Verwalten von Passwortrichtlinien

Eine Passwortrichtlinie ist eine Sammlung von vom Administrator festgelegten Regeln, die die Kriterien für das Erstellen und Ersetzen von Endbenutzerpasswörtern festlegen. NMAS ermöglicht das Erzwingen von Passwortrichtlinien, die Sie Benutzern in eDirectory zuweisen. Passwortrichtlinien können auch Selbstbedienungsfunktionen für vergessene Passwörter enthalten, die dazu beitragen, die Anzahl der Helpdeskanrufe für vergessene Passwörter zu reduzieren. Eine weitere Selbstbedienungsfunktion steht zum Zurücksetzen von Passwörtern zur Verfügung. Sie bietet dem Benutzer die Möglichkeit, sein Passwort zu ändern, und zeigt die vom Administrator in der Passwortrichtlinie festgelegten Regeln an. Die Benutzer greifen über die Identity Manager-Benutzeranwendung oder über Identity Console auf diese Funktionen zu.

Mit dem Passwortrichtlinienmodul können Sie die folgenden Aufgaben ausführen:

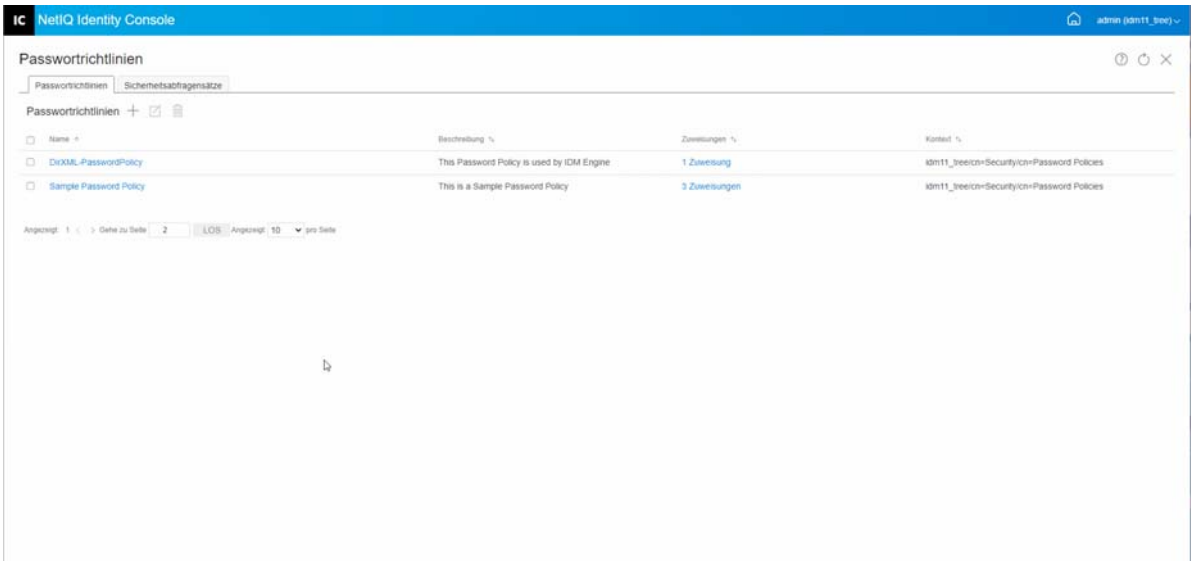
- „Passwortrichtlinien mit Standardeinstellungen erstellen“, auf Seite 118
- „Passwortrichtlinien mit benutzerdefinierten Einstellungen erstellen“, auf Seite 118
- „Passwortrichtlinien ändern“, auf Seite 122
- „Passwortrichtlinien löschen“, auf Seite 122

Passwortrichtlinien mit Standardeinstellungen erstellen

Führen Sie zum Erstellen einer neuen Passwortrichtlinie die folgenden Schritte aus:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Passwortrichtlinien**.
2. Klicken Sie auf das Symbol +, um eine neue Passwortrichtlinie zu erstellen.
3. Geben Sie im nächsten Bildschirm den Namen, den Kontext, die Beschreibung und eine Passwortänderungsmeldung an.
4. Wenn Sie eine Passwortrichtlinie mit den Standardeinstellungen erstellen möchten, aktivieren Sie das Kontrollkästchen **Neue Passwortrichtlinie basierend auf den Standardeinstellungen erstellen** und klicken Sie auf **Weiter**, um die Seite **Zusammenfassung** anzuzeigen.
5. Überprüfen Sie die Details auf der Seite **Zusammenfassung** und klicken Sie auf **Erstellen**.
6. Eine Meldung bestätigt die erfolgreiche Erstellung der Passwortrichtlinie.

Abbildung 18-9 *Passwortrichtlinien mit Standardeinstellungen erstellen*



Passwortrichtlinien mit benutzerdefinierten Einstellungen erstellen

Führen Sie die folgenden Schritte aus, um eine Passwortrichtlinie mit benutzerdefinierten Einstellungen zu erstellen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Passwortrichtlinien**.
2. Klicken Sie auf das Symbol +, um eine neue Passwortrichtlinie zu erstellen.
3. Geben Sie im nächsten Bildschirm den Namen, den Kontext, die Beschreibung und eine Passwortänderungsmeldung an.
4. Wenn Sie eine Passwortrichtlinie mit den benutzerdefinierten Einstellungen erstellen möchten, klicken Sie auf **Weiter**.

5 Führen Sie auf der Seite **Konfiguration** die folgenden Aktionen aus:

5a **Universelles Passwort aktivieren:** Die Aktivierung des universellen Passworts für eine Richtlinie ermöglicht Ihnen, Optionen der Funktion "Passwortrichtlinien" zu verwenden. Das universelle Passwort für eine Richtlinie kann jedoch erst aktiviert werden, wenn die Voraussetzungen für universelle Passwörter in der Umgebung erfüllt sind.

5b **Regeln für erweitertes Passwort aktivieren:** Mit dieser Option werden die Passwortregeln aktiviert, die sich unter Erweiterte Passwortregeln befinden. Diese Regeln helfen Ihnen, Ihre Umgebung zu schützen, indem sie Ihnen die Kontrolle über Kriterien wie die Lebensdauer oder den Inhalt der Passwörter gibt. Sie können beispielsweise festlegen, welche Art von Kombination aus Buchstaben, Zahlen, Groß- oder Kleinbuchstaben und Sonderzeichen das Passwort enthalten muss. Passwörter, die Ihrer Meinung nach nicht sicher sind (beispielsweise der Firmenname), können ausgeschlossen werden.

5c **Passwortsynchronisierung:** Mit diesen Optionen wird die Synchronisierung des universellen Passworts in eDirectory mit anderen Arten von Identitätsdepot-Passwörtern definiert. Die Passwortsynchronisierung enthält die folgenden Optionen:

5c1 **NDS-Passwort beim Festlegen des Passworts entfernen:** Bei aktivierter Option wird das NDS-Passwort deaktiviert, wenn das universelle Passwort eingerichtet wird. Die Benutzer können keine älteren Methoden oder Dienstprogramme verwenden, die sich direkt mit dem NDS-Passwort anmelden, statt mit NMAS zu kommunizieren. Wenn diese Option aktiviert ist, wird die nächste Option **NDS-Passwort beim Festlegen des Passworts synchronisieren** standardmäßig deaktiviert.

5c2 **NDS-Passwort beim Festlegen des Passworts synchronisieren:** Wenn diese Option aktiviert ist, wird bei der Einrichtung des universellen Passworts in Anwendungen wie Identity Console auch das NDS-Passwort geändert.

5c3 **Einfaches Passwort beim Festlegen des Passworts synchronisieren:** Diese Option ermöglicht die Kompatibilität mit NetIQ und Clients von Drittanbietern, die einfache Passwörter und Benutzerbereitstellung verwenden.

5c4 **Verteilungspasswort beim Festlegen des Passworts synchronisieren:** Mit dieser Option wird festgelegt, ob die Metaverzeichnis-Engine das universelle Passwort eines Benutzers in eDirectory abrufen oder festlegen kann.

5d **Abruf des universellen Passworts:** Folgende Optionen stehen zur Auswahl:

5d1 **Abrufen des Passworts durch Benutzer zulassen:** Lässt das Abrufen des Passworts durch den Benutzeragenten zu. Mit dieser Option wird festgelegt, ob die Selbstbedienungsfunktion "Vergessenes Passwort" ein Passwort im Namen des Benutzers abrufen kann, sodass das Passwort per Email an den Benutzer gesendet werden kann. Bei deaktivierter Option ist die entsprechende Funktion auf der Registerkarte "Passwort vergessen" in der Passwortrichtlinie abgeblendet.

5d2 **Abrufen von Passwörtern durch Administrator zulassen:** Aktivieren Sie diese Option, wenn Sie von einem Service benötigt wird. In Identity Manager ist es nicht erforderlich, dass Kennwörter von Administratoren abgerufen werden. Für bestimmte Services von Drittanbietern kann diese Option jedoch hilfreich sein.

5d3 **Zulassen, dass folgende Personen Passwörter abrufen:** Wählen Sie den entsprechenden Benutzer aus, der das Passwort abrufen können soll, indem Sie auf das Symbol + klicken.

5e Authentifizierung:

5e1 Überprüfen, ob vorhandene Passwörter die Passwortrichtlinie erfüllen (Überprüfung erfolgt bei der Anmeldung): Diese Option ist hilfreich, wenn Sie eine neue Passwortrichtlinie verteilen oder die erweiterten Passwortregeln für eine vorhandene Richtlinie ändern und sicherstellen möchten, dass die vorhandenen Passwörter den neuen bzw. geänderten Regeln entsprechen.

Wenn Sie diese Option auswählen, werden die vorhandenen Passwörter von Benutzern bei der Anmeldung überprüft, um sicherzustellen, dass sie mit den erweiterten Passwortregeln in der neuen oder geänderten Passwortrichtlinie übereinstimmen. Ist ein vorhandenes Passwort nicht kompatibel, muss der Benutzer das Passwort ändern.

Wenn Sie fertig sind, klicken Sie auf **Weiter**.

6 **Erweiterte Passwortregeln** helfen Ihnen, Ihre Umgebung zu schützen, indem sie Ihnen die Kontrolle über Kriterien wie die Lebensdauer des Passworts, die erforderliche Passwortänderungsfrequenz oder die Art der enthaltenen Zeichen gibt.

Sonderzeichen sind Zeichen, die keine Zahlen (0-9) oder Buchstaben sind.

Auf der Seite „Erweiterte Passwortregeln“ können Sie die folgenden Aktionen ausführen:

6a Sie können mit der Microsoft-Komplexitätsrichtlinie (vor Microsoft Windows Server 2008), der Microsoft Server 2008-Kennwortrichtlinie oder der Novell-Syntax Passwortsyntaxeinstellungen verwalten.

6b Geben Sie im Assistenten die erforderlichen Optionen für „Passwort ändern“, „Gültigkeitsdauer des Passworts“, „Passwortlänge und -zusammensetzung“ und „Passwortausschlüsse“ an und klicken Sie auf **Weiter**.

7 Durch Aktivieren der Selbstbedienungsfunktion **Passwort vergessen** für Benutzer, die ihr Passwort vergessen haben, können Sie Helpdesk-Kosten reduzieren. Diese Selbstbedienungsfunktionen stehen Benutzern über das Identity Console-Portal zur Verfügung. Auf der Seite „Passwort vergessen“ können Sie die folgenden Aktionen ausführen:

HINWEIS: Wenn Sie „Passwort vergessen“ aktivieren, müssen Sie außerdem festlegen, ob ein Sicherheitsabfragensatz erforderlich ist, um den Benutzer bei der Anmeldung zu unterstützen.

7a Herausforderungssätze: Wenn Sie Sicherheitsabfragensätze verwenden, können die Benutzer die Selbstbedienungsfunktion „Passwort vergessen“ erst verwenden, nachdem sie die Sicherheitsfragen beantwortet haben. Um sicherzustellen, dass die Benutzer zur Eingabe dieser Informationen über das Identity Console-Portal aufgefordert werden, aktivieren Sie die Option **Sicherheitsabfragensatz erfordern**.

7b Aktion: Die verfügbaren Optionen auf dieser Registerkarte umfassen das Zurücksetzen des Passworts mithilfe von Sicherheitsabfragesätzen und eines universellen Passworts, das Senden des aktuellen Passworts oder des Passworthinweises per Email und das Anzeigen des Passworthinweises.

7c Authentifizieren: Aktivieren Sie das Kontrollkästchen **Benutzer bei der Authentifizierung zwingen, Sicherheitsfragen und/oder Hinweise zu konfigurieren**, um sicherzustellen, dass die Benutzer aufgefordert werden, Sicherheitsabfragensätze oder einen Passworthinweis anzugeben.

Wenn Sie fertig sind, klicken Sie auf **Weiter**.

8 Eine Richtlinie wird erst dann wirksam, wenn sie mindestens einem Objekt zugewiesen wird. Es empfiehlt sich, Richtlinien auf einer möglichst hohen Ebene im Baum zuzuweisen, um die Administration zu vereinfachen. Eine Passwortrichtlinie kann den folgenden Objekten zugewiesen werden:

8a **Objekt „Login Policy“:** Es wird empfohlen, eine Standardpasswortrichtlinie für alle Benutzer im Baum zu erstellen und dem Anmelderichtlinienobjekt zuzuweisen, das sich im Sicherheitscontainer befindet.

8b **Container, der Partitionsstamm ist:** Wenn Sie einem Container eine Richtlinie zuweisen, der als Stamm einer Partition fungiert, wird die Richtlinienzuweisung an alle Benutzer in dieser Partition vererbt, einschließlich der Benutzer in den Untercontainern.

8c **Container, der nicht als Partitionsstamm fungiert:** Wenn Sie einem Container, der nicht als Stamm einer Partition fungiert, eine Richtlinie zuweisen, wird die Richtlinienzuweisung nur an die Benutzer vererbt, die sich in diesem Container befinden. Die Richtlinie wird nicht an Benutzer vererbt, die sich in Untercontainern befinden.

Soll die Richtlinie für alle Benutzer unterhalb eines nicht als Partitionsstamm fungierenden Containers gelten, muss die Richtlinie jedem Untercontainer einzeln zugewiesen werden.

8d **Benutzer:** Eine Richtlinie kann einem oder mehreren Benutzern zugewiesen werden.

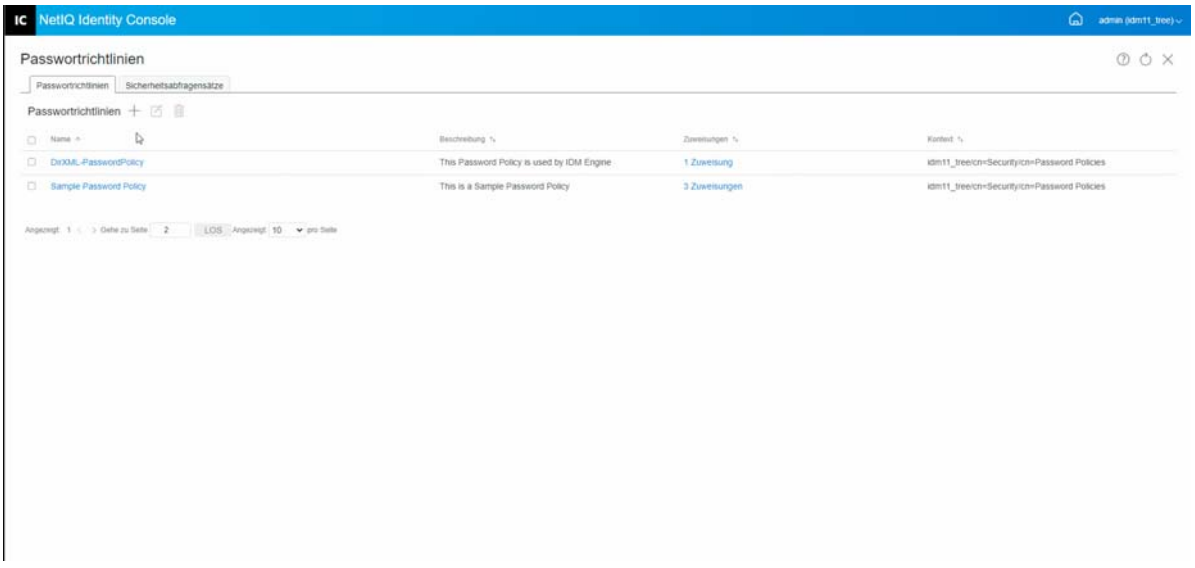
Um eine Richtlinie zuzuweisen, klicken Sie auf das Symbol +. Wählen Sie dann durch Durchsuchen das entsprechende Objekt aus, um eine Passwortrichtlinie zuzuweisen.

Falls Sie eine Richtlinienverknüpfung entfernen möchten, wählen Sie die Richtlinie aus der Liste aus und klicken Sie auf das Symbol 🗑.

9 Überprüfen Sie die Details auf der Seite **Zusammenfassung** und klicken Sie auf **Erstellen**.

10 Eine Meldung bestätigt die erfolgreiche Erstellung der Passwortrichtlinie.

Abbildung 18-10 *Passwortrichtlinien mit benutzerdefinierten Einstellungen erstellen*

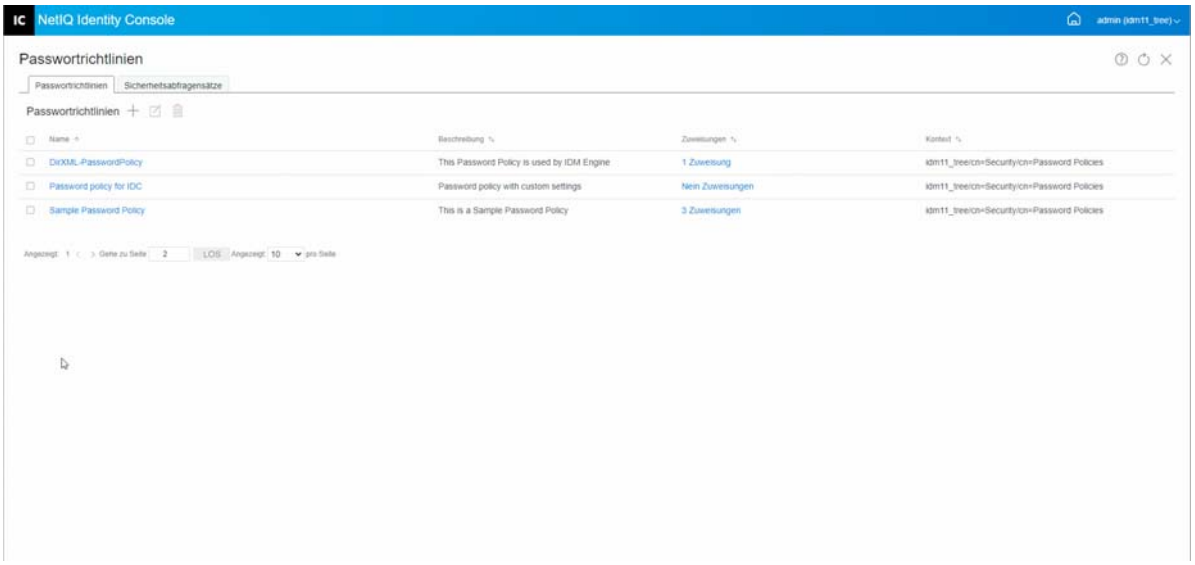


Passwortrichtlinien ändern

Führen Sie die folgenden Schritte aus, um eine vorhandene Passwortrichtlinie zu ändern:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Passwortrichtlinien**.
2. Wählen Sie die geeignete Passwortrichtlinie aus der Liste aus und klicken Sie auf das Symbol ☑.
3. Nehmen Sie die erforderlichen Änderungen auf der Seite **Passwortrichtlinie ändern** vor und klicken Sie auf **Speichern**.

Abbildung 18-11 *Passwortrichtlinien ändern*

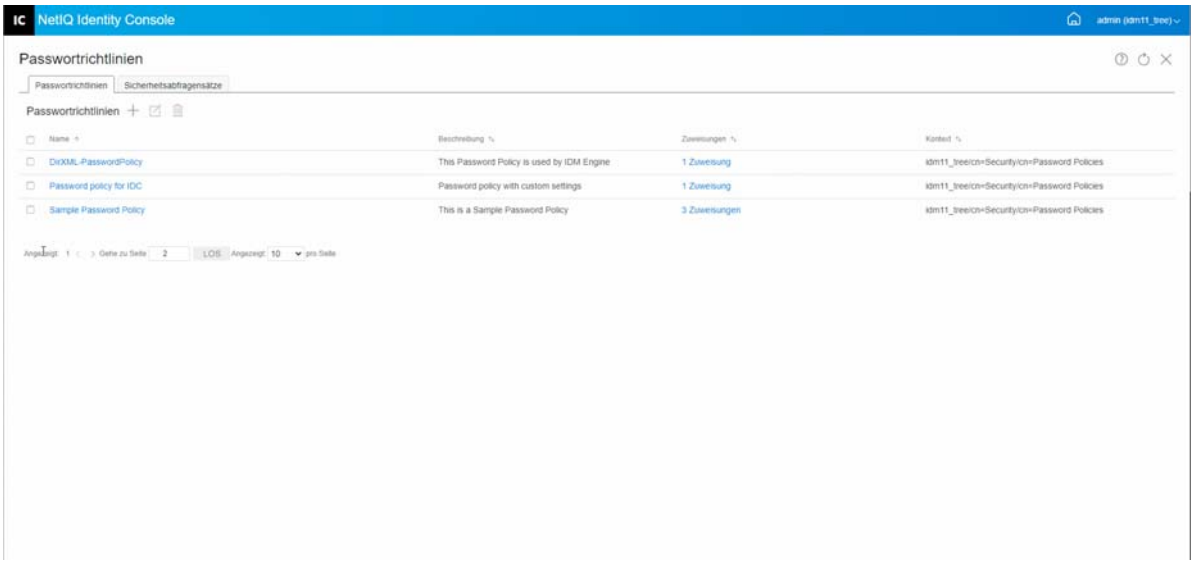


Passwortrichtlinien löschen

Führen Sie die folgenden Schritte aus, um Passwortrichtlinien zu löschen:

1. Klicken Sie auf der Identity Console-Landeseite auf die Optionen **Authentifizierungsverwaltung** > **Passwortrichtlinien**.
2. Wählen Sie die geeigneten Passwortrichtlinien aus der Liste aus und klicken Sie auf das Symbol 🗑.
3. Klicken Sie im daraufhin angezeigten Warnbildschirm auf **OK**.
4. Eine Meldung bestätigt das Löschen der Passwortrichtlinien.

Abbildung 18-12 *Löschen einer Passwortrichtlinie*



Sicherheitsabfragensätze verwalten

Ein Herausforderungssatz besteht aus einer oder mehreren Fragen, die ein Benutzer zur Validierung seiner Identität beantworten muss. Ein Herausforderungssatz ist Teil des Passwort-Selbsbedienungsfunktion.

Wenn Benutzer Probleme haben, sich das Kennwort zu merken oder es zu verwenden, können sie die Passwort-Selbstbedienung verwenden, statt sich an das Helpdesk zu wenden. Mit einem Herausforderungssatz kann ein Benutzer seine Identität validieren und anschließend einen Hinweis oder das Passwort in einer Email erhalten oder ein Passwort über einen Browser zurücksetzen.

Sie können festlegen, dass Benutzer ihre eigenen Fragen erstellen und beantworten können bzw. von Ihnen erstellte Fragen beantworten müssen.

Mit der Seite "Herausforderungssätze" können Sie nach vorhandenen Herausforderungssätzen suchen, neue Herausforderungssätze erstellen und vorhandene Herausforderungssätze bearbeiten.

- „Neue Sicherheitsabfragensätze erstellen“, auf Seite 123
- „Sicherheitsabfragensätze ändern“, auf Seite 124
- „Sicherheitsabfragensätze löschen“, auf Seite 125

Neue Sicherheitsabfragensätze erstellen

Führen Sie zum Erstellen eines neuen Sicherheitsabfragensatzes die folgenden Schritte aus:

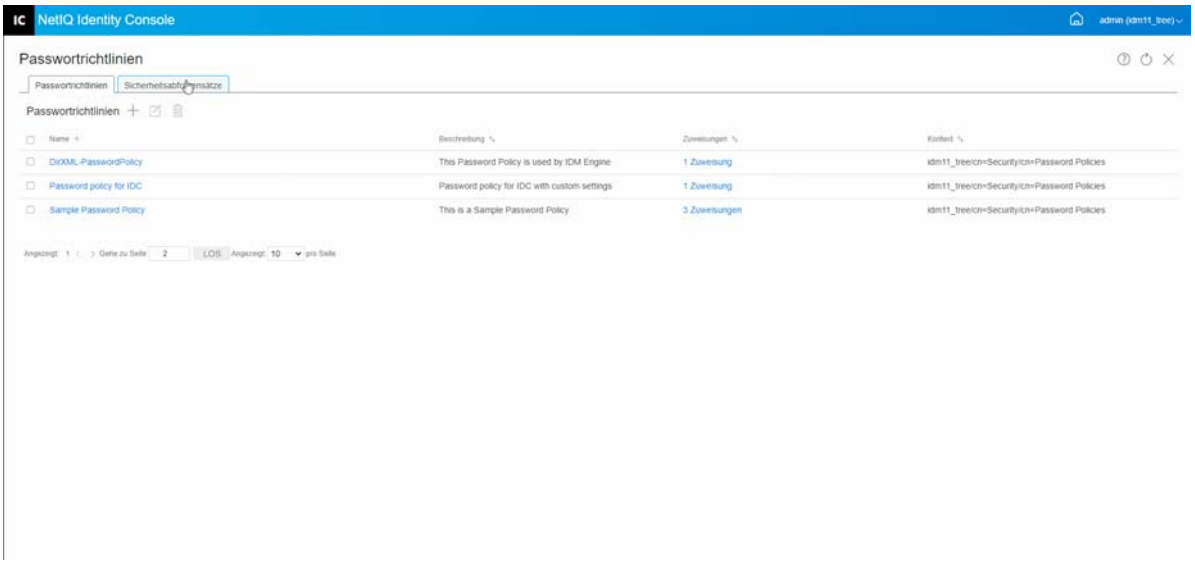
1. Klicken Sie auf der Identity Console-Landeseite auf **Authentifizierungsverwaltung** > **Passwortrichtlinien** > **Sicherheitsabfragensätze**.
2. Klicken Sie auf das Symbol +, um einen neuen Sicherheitsabfragensatz zu erstellen.
3. Geben Sie einen Namen für das Sicherheitsabfragensatzobjekt an und wählen Sie den Container oder Untercontainer aus, in dem der Sicherheitsabfragensatz erstellt werden soll.

4 Erstellen Sie einen neuen Satz von Fragen, die zum Abrufen des Passworts des Benutzers gestellt werden sollen. Sie können auch aus dem vorhandenen Satz zufälliger Fragen auswählen.

5 Legen Sie die Anzahl der zu stellenden Fragen fest und klicken Sie auf **Erstellen**.

6 Eine Meldung bestätigt die erfolgreiche Erstellung des Sicherheitsabfragensatzes.

Abbildung 18-13 *Erstellen von Herausforderungssätzen*



Sicherheitsabfragensätze ändern

Führen Sie die folgenden Schritte aus, um einen vorhandenen Sicherheitsabfragensatz zu ändern:

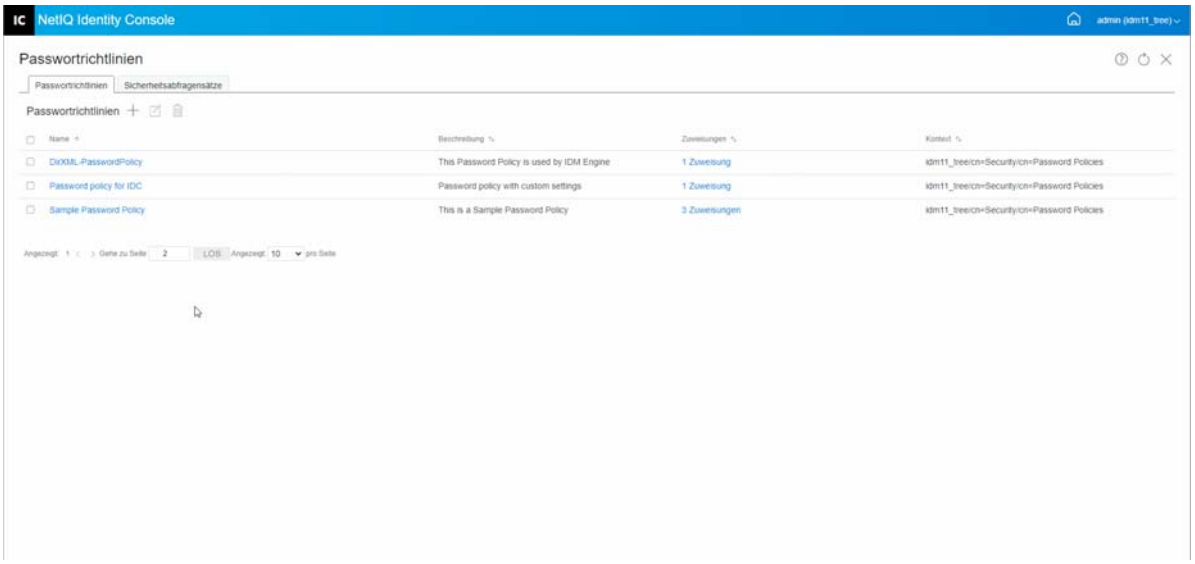
1 Klicken Sie auf der Identity Console-Landeseite auf **Authentifizierungsverwaltung** > **Passwortrichtlinien** > **Sicherheitsabfragensätze**.

2 Wählen Sie den entsprechenden Sicherheitsabfragensatz aus der Liste aus und klicken Sie auf das Symbol ☑.

3 Nehmen Sie auf der Seite „Sicherheitsabfragensatz ändern“ die erforderlichen Änderungen vor und klicken Sie auf **Speichern**.

4 Eine Meldung bestätigt das erfolgreiche Ändern des Sicherheitsabfragensatzes.

Abbildung 18-14 *Sicherheitsabfragensätze ändern*

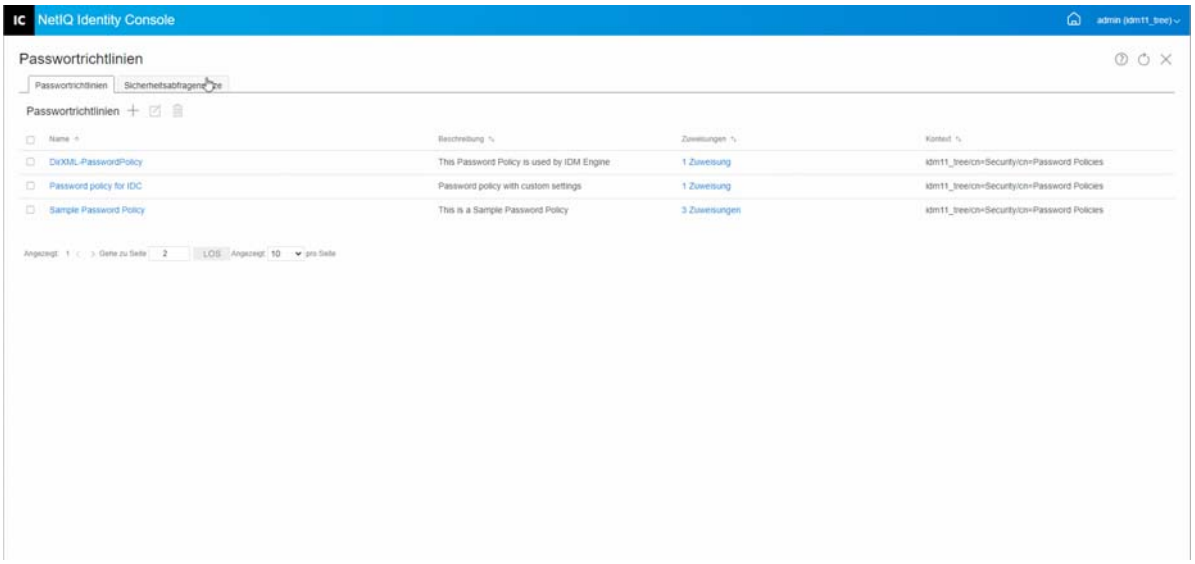


Sicherheitsabfragensätze löschen

Führen Sie die folgenden Schritte aus, um einen Sicherheitsabfragensatz zu löschen:

1. Klicken Sie auf der Identity Console-Landeseite auf **Authentifizierungsverwaltung** > **Passwortrichtlinien** > **Sicherheitsabfragensätze**.
2. Wählen Sie den erforderlichen Sicherheitsabfragensatz aus der Liste aus und klicken Sie auf das Symbol .
3. Klicken Sie auf dem Bestätigungsbildschirm auf **OK**.
4. Eine Meldung bestätigt die erfolgreiche Löschung des Sicherheitsabfragensatzes.

Abbildung 18-15 *Sicherheitsabfragensatz löschen*



19 SNMP-Gruppenobjekte verwalten

SNMP (Simple Network Management Protocol) ist das Standardbetriebs- und -wartungsprotokoll für den Austausch im Internet von Verwaltungsinformationen zwischen Verwaltungskonsolenanwendungen und verwalteten Geräten.

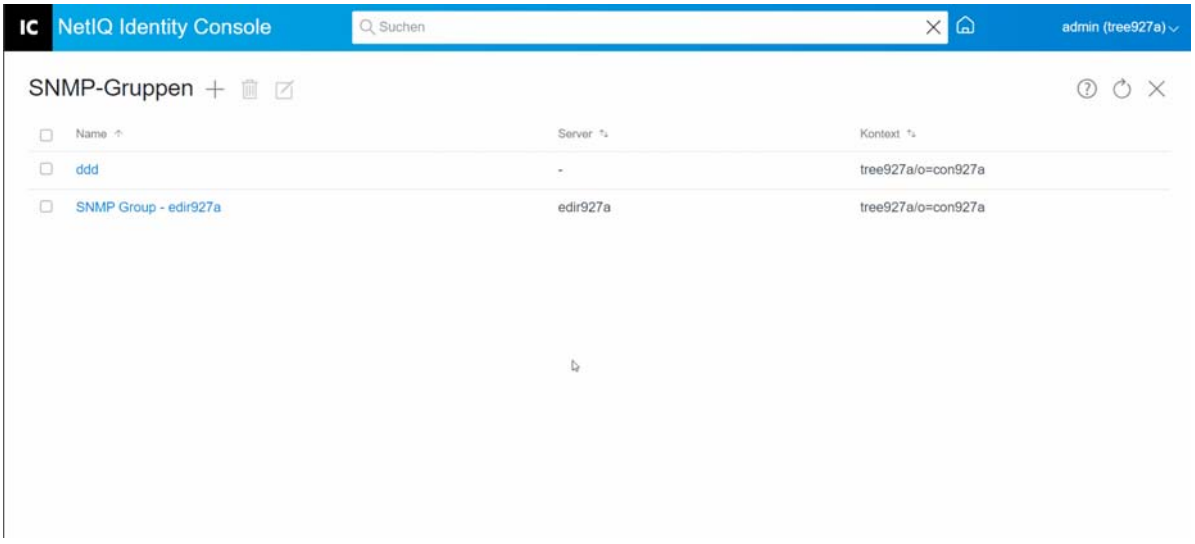
Mit dem SNMP-Modul können Sie die folgenden Aufgaben ausführen:

SNMP-Gruppenobjekte erstellen

Führen Sie die folgenden Schritte aus, um SNMP-Gruppenobjekte zu erstellen:

1. Klicken Sie auf der Identity Console-Landeseite auf das Modul **SNMP**.
2. Klicken Sie auf das Symbol +, um ein neues SNMP-Gruppenobjekt zu erstellen.
3. Geben Sie den Namen an und wählen Sie den Kontext aus, um ein neues SNMP-Gruppenobjekt zu erstellen.
4. Klicken Sie auf die Schaltfläche **Erstellen**.
5. Eine Meldung bestätigt die erfolgreiche Erstellung des SNMP-Gruppenobjekts.

Abbildung 19-1 *SNMP-Gruppenobjekte erstellen*

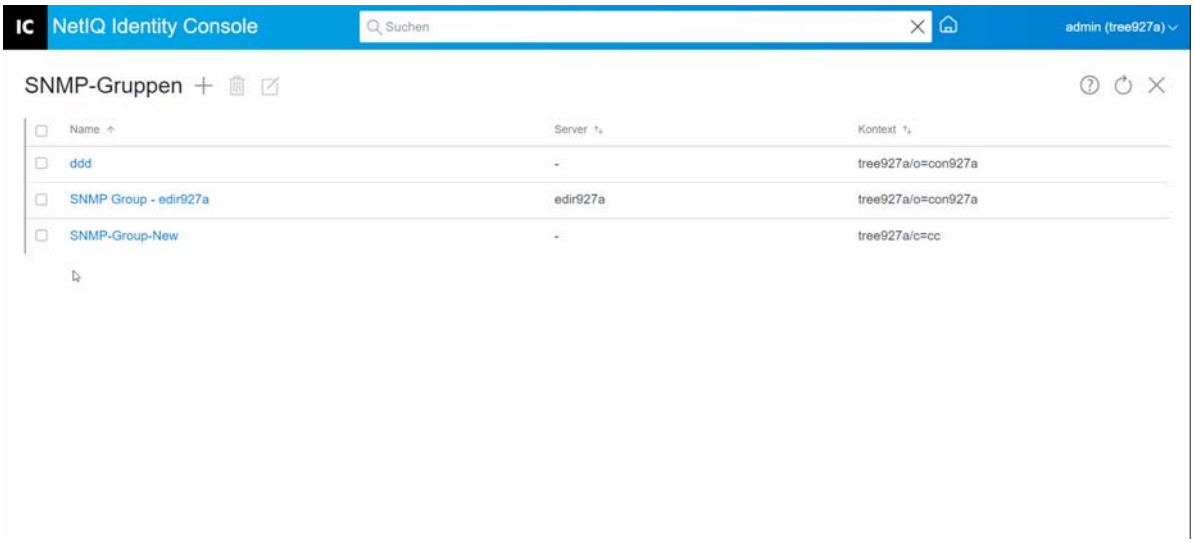


SNMP-Gruppenobjekte ändern

Führen Sie die folgenden Schritte aus, um SNMP-Gruppenobjekte zu ändern:

1. Klicken Sie auf der Identity Console-Landeseite auf das Modul **SNMP**.
2. Wählen Sie das SNMP-Gruppenobjekt aus, das Sie ändern möchten, und klicken Sie auf das Symbol .
3. Ändern Sie die konfigurierbaren Parameter auf der Seite **Allgemein**/**Traps**.
4. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche **Speichern**.
5. Eine Meldung bestätigt die erfolgreiche Änderung des SNMP-Gruppenobjekts.

Abbildung 19-2 *SNMP-Gruppenobjekte ändern*

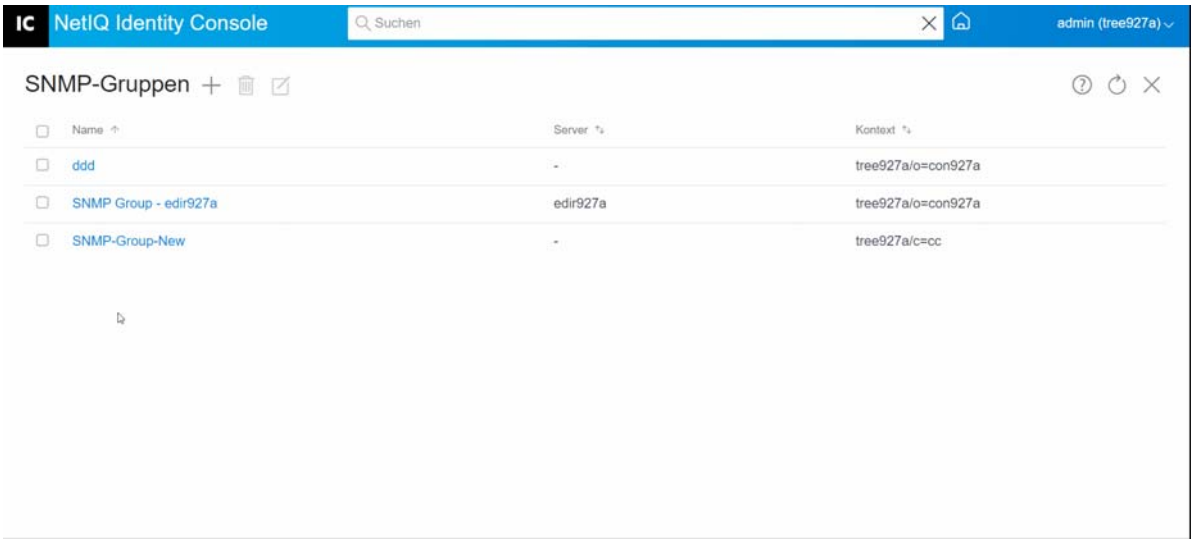


SNMP-Gruppenobjekte löschen

Führen Sie die folgenden Schritte aus, um SNMP-Gruppenobjekte zu löschen:

1. Klicken Sie auf der Identity Console-Landeseite auf das Modul **SNMP**.
2. Wählen Sie das SNMP-Gruppenobjekt aus, das Sie ändern möchten, und klicken Sie auf das Symbol .
3. Klicken Sie im nächsten Bildschirm auf **OK**.
4. Eine Meldung bestätigt die erfolgreiche Löschung des SNMP-Gruppenobjekts.

Abbildung 19-3 *SNMP-Gruppenobjekte löschen*



20 Enhanced Background Authentication verwalten

Um über das EBA-Plugin von Identity Console auf eDirectory zugreifen zu können, muss in Ihrem Baum ein EBA-fähiger Server mit einer gültigen eba.p12-Datei vorhanden sein. Weitere Informationen zur Aktivierung von EBA in Ihrem eDirectory-Baum finden Sie unter Enabling EBA on an eDirectory Tree (EBA in einem eDirectory-Baum aktivieren) im *NetIQ eDirectory Administration Guide* (NetIQ eDirectory-Administrationshandbuch).

HINWEIS: Wenn Sie das EBA-Modul mit Identity Console verwenden möchten, müssen Sie Ihren eDirectory-Server auf 9.2.4 HF2 aufrüsten.

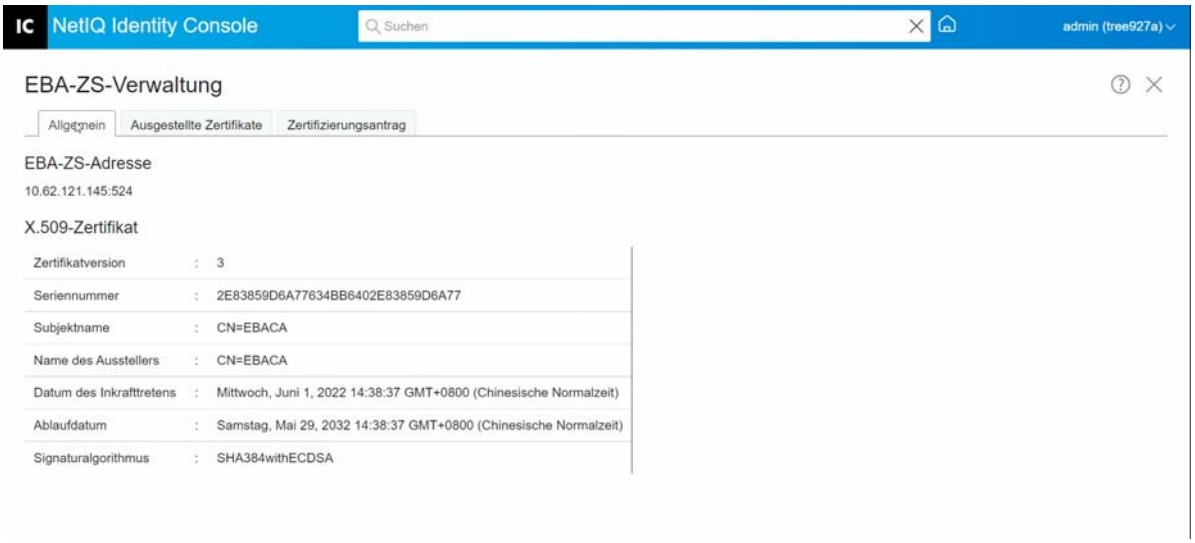
Um die Seite „EBA-ZS-Verwaltung“ zu öffnen, melden Sie sich beim Identity Console-Portal an und klicken Sie auf das Modul **EBA**.

Die Seite „EBA-ZS-Verwaltung“ enthält die folgenden Registerkarten zur Verwaltung verschiedener Aspekte der EBA-Zertifizierungsstelle:

- **Allgemein:** Zeigt die IP-Adresse der EBA-Zertifizierungsstelle und das Zertifikat an.
- **Ausgestellte Zertifikate:** Zeigt die Zertifikate der NCP-Zertifizierungsstelle zusammen mit ihrer IP-Adresse und dem Port an.

  Um ein Zertifikat zu widerrufen, wählen Sie es aus und klicken Sie auf ⊘. Verwenden Sie diese Option nur in extremen Situationen, weil der Server, der das NCP-ZS-Zertifikat besitzt, nicht mehr funktionsfähig wird, wenn Sie das Zertifikat widerrufen. In der Regel ist das Widerrufen des Zertifikats erforderlich, wenn ein Server kompromittiert ist.
- **Zertifizierungsantrag:** Listet die Zertifizierungsanträge mit ausstehender Administratorgenehmigung auf. Um einen Zertifizierungsantrag zu genehmigen, wählen Sie das Zertifikat in der Liste aus und klicken Sie auf **Genehmigen**.

Abbildung 20-1 *Enhanced Background Authentication verwalten*



II Verwalten von Identity Manager mit Identity Console

Dieser Abschnitt beschreibt verschiedene Aufgaben, die Sie zum Verwalten Ihrer Identity Manager-Server mit dem Identity Console-Portal ausführen können.

21 Treiber und Treibersätze verwalten

Ein Treibersatz ist ein Container, der Identity Manager-Treiber enthält. Auf einem Server kann immer nur ein Treibersatz aktiv sein. Aus diesem Grund müssen alle aktiven Treiber im selben Treibersatz zusammengefasst werden. Ein Treibersatz kann mit dem Designer-Werkzeug erstellt werden. Weitere Informationen finden Sie unter Konfigurieren von Treibersätzen im *Administrationshandbuch zu NetIQ Designer für Identity Manager*.

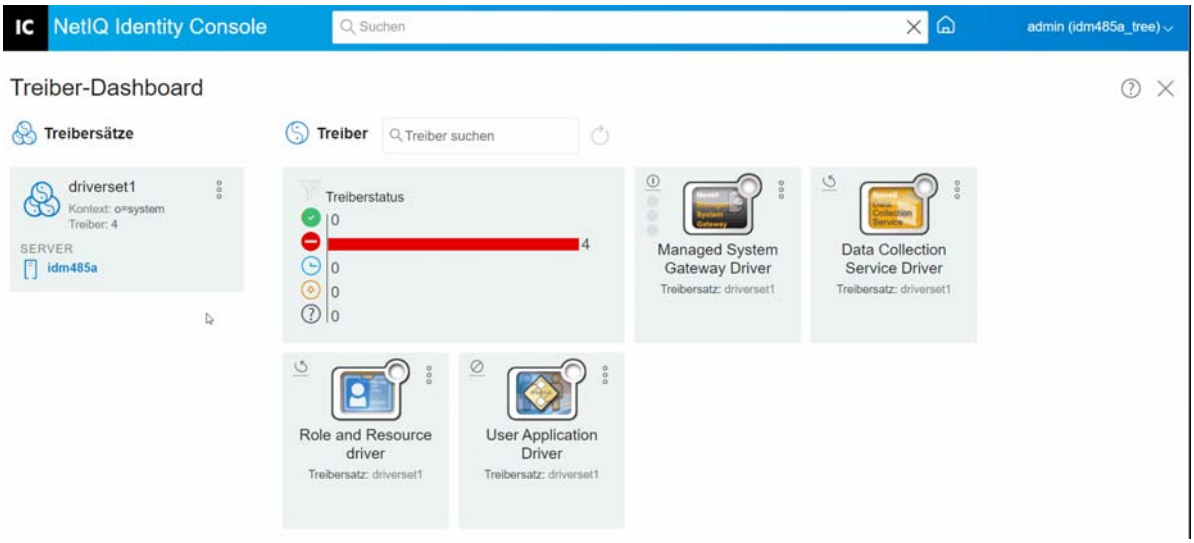
Server hinzufügen oder löschen

Ein Treibersatz kann mit einem oder mit mehreren Servern gleichzeitig verknüpft sein. Je nach Ihren Anforderungen können Sie jedoch ein anderes Treibersatzobjekt mit dem verfügbaren Server verknüpfen.

Um einen neuen Server hinzuzufügen, klicken Sie auf das Symbol auf dem jeweiligen Treibersatzobjekt > wählen Sie **Server hinzufügen** aus und wählen Sie den entsprechenden Server im Kontextbrowser aus.

Um einen vorhandenen Server zu löschen, wählen Sie die Option **Server entfernen** aus.

Abbildung 21-1 *Server zu einem Treibersatz hinzufügen*



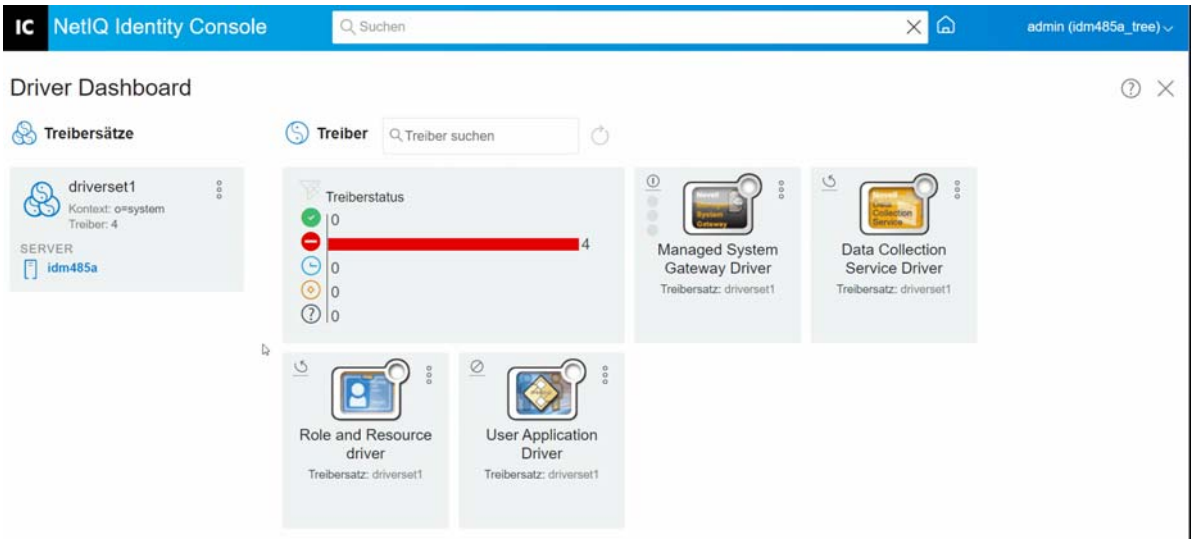
Treibersätze mit dem Produktaktivierungsschlüssel aktivieren

Bevor Sie einen Treibersatz und die darin enthaltenen Treiber verwenden, müssen Sie den Treibersatz mit dem Aktivierungscode aktivieren, den Sie mit Ihrer Email-ID empfangen haben. Nach dem Kauf einer Lizenz erhalten Sie Ihren Aktivierungsschlüssel von NetIQ. Führen Sie die folgenden Schritte aus, um den Treibersatz mit dem Aktivierungsschlüssel zu aktivieren:

1. Klicken Sie auf dem Identity Console-Startbildschirm auf die Registerkarte **IDM-Administration**.
2. Klicken Sie auf das Aktionssymbol im Feld des Treibersatzes, den Sie aktivieren möchten, und klicken Sie auf **Aktivierungsinstallation**.

   Beim Anwenden der Aktivierung werden auf jeder Treibersatz-Registerkarte in der IDM-Administrationskachel die Aktivierungsinformationen für alle Server angezeigt, die diesem Treibersatz zugeordnet sind. Anhand dieser Informationen können Sie ermitteln, wann die Aktivierung abläuft.
3. Wenn Sie die Aktivierungsdatei auf Ihren Computer heruntergeladen haben, aktivieren Sie das Kontrollkästchen **Eine Datei auswählen, die den Berechtigungsnachweis enthält**.
4. Wählen Sie durch Durchsuchen die Aktivierungsdatei aus und klicken Sie auf **Senden**.
5. Alternativ können Sie den Treibersatz mit dem Inhalt der Aktivierungsdatei aktivieren. Aktivieren Sie das Kontrollkästchen für **Berechtigungsnachweis eingeben**.
   - **5a** Öffnen Sie die Datei mit der Produktaktivierungsberechtigung und kopieren Sie ihren Inhalt in die Zwischenablage.
   - **5b** Wenn Sie den Inhalt kopieren, fügen Sie keine zusätzlichen Zeilen oder Leerzeichen ein. Kopieren Sie den Text vom ersten Bindestrich (-) des Berechtigungsnachweises (----BEGINN DER PRODUKTAKTIVIERUNGSBERECHTIGUNG) bis zum letzten Bindestrich (-) der Berechtigung (ENDE DER PRODUKTAKTIVIERUNGSBERECHTIGUNG-----) und klicken Sie auf **Fertigstellen**.
6. Eine Meldung bestätigt die erfolgreiche Aktivierung des Treibersatzes.

Abbildung 21-2 *Treibersätze aktivieren*

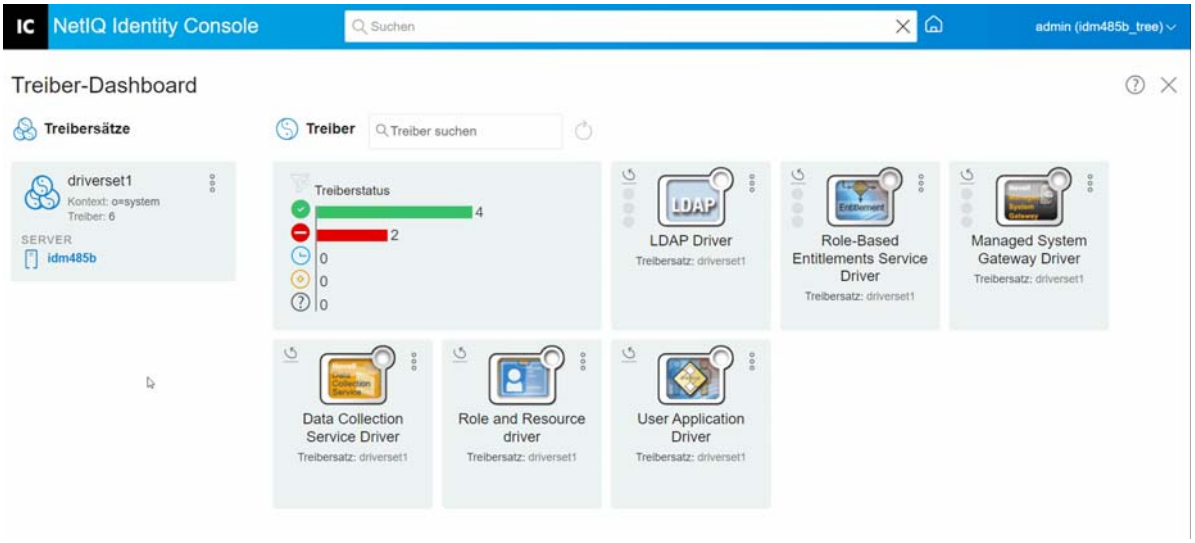


Aktivierungsinformationen von Treibersätzen anzeigen

Nach der Aktivierung des Treibersatzes müssen Sie überprüfen, ob der Treibersatz erfolgreich aktiviert wurde. Führen Sie hierzu die folgenden Schritte aus:

1. Klicken Sie auf dem Identity Console-Startbildschirm auf die Registerkarte **IDM-Administration**.
2. Klicken Sie auf das Aktionssymbol ⋮ im spezifischen Treibersatzobjekt, für das Sie die Aktivierungsinformationen überprüfen möchten, und klicken Sie auf **Aktivierungsinformationen**.
3. Ein Popup-Fenster Informationen mit den Informationen zur Aktivierung wird auf Ihrem Computer angezeigt. Sie können die Aktivierungsdetails des jeweiligen Treibersatzes auf dieser Seite überprüfen.

Abbildung 21-3 *Aktivierungsinformationen von Treibersätzen anzeigen*

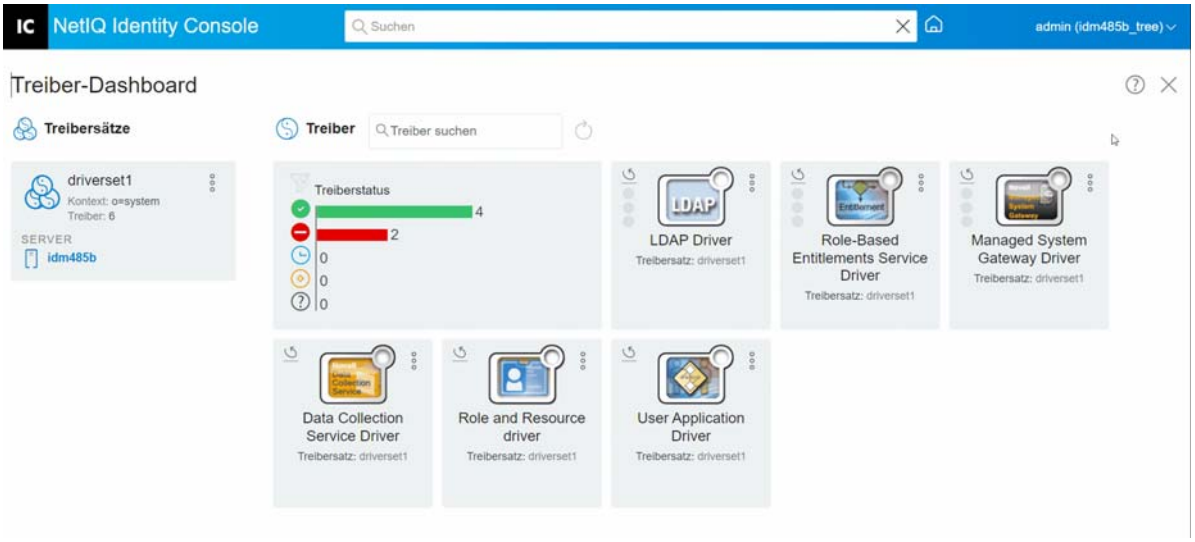


Treiber starten und stoppen

Ein Treiber ist nach der Erstellung standardmäßig gestoppt. Damit der Treiber funktioniert, müssen Sie den Treiber starten. Identity Manager ist ein ereignisgesteuertes System. Das bedeutet, dass der Treiber nach dem Starten im Leerlauf bleibt, bis ein Ereignis eintritt. Führen Sie die folgenden Schritte aus, um einen Treiber zu starten oder zu stoppen.

1. Klicken Sie auf dem Identity Console-Startbildschirm auf die Registerkarte **IDM-Administration**.
2. Klicken Sie auf das jeweilige Treibersatzobjekt auf der rechten Seite des Computerbildschirms, um alle damit verknüpften Treiber anzuzeigen.
3. Klicken Sie auf das Aktionssymbol für den jeweiligen Treiber und wählen Sie **Treiber starten** aus.
4. Um ein Treiberobjekt zu stoppen, klicken Sie auf das Aktionssymbol für den jeweiligen Treiber und wählen Sie **Treiber stoppen** aus.
5. (Optional) Alternativ können Sie alle Treiber im gleichen Treibersatzobjekt gleichzeitig starten oder stoppen. Klicken Sie auf das Aktionssymbol im Treibersatzobjekt und wählen Sie **Alle Treiber starten** oder **Alle Treiber stoppen** aus.

Abbildung 21-4 *Treiber starten und stoppen*



Treiber suchen

Identity Console bietet die Möglichkeit, nach einem bestimmten Treiber auf dem Server zu suchen. Führen Sie die folgenden Schritte aus, um nach einem Treiber zu suchen:

1. Klicken Sie auf dem Identity Console-Startbildschirm auf die Registerkarte **IDM-Administration**.
2. Geben Sie den Namen des Treibers im Feld **Suchen** an. Das spezifische Treiberobjekt wird auf dem Computerbildschirm angezeigt. Sie können die Liste der Treiber auch aktualisieren, indem Sie auf das Symbol klicken.

Abbildung 21-5 *Treiber suchen*

Treiber und Treibersätze filtern

Die Treiber können basierend auf ihrem Status auf der Seite **IDM-Administration** gefiltert werden. So filtern Sie Treiber:

1. Klicken Sie auf dem Identity Console-Startbildschirm auf die Registerkarte **IDM-Administration**.
2. Klicken Sie auf der Kachel zum **Treiberstatus** auf die folgenden Symbole, um Treiber basierend auf ihrem Status herauszufiltern:
   - Klicken Sie auf das Symbol , um alle ausgeführten Treiber auf dem Server zu filtern.
   - Klicken Sie auf das Symbol , um alle gestoppten Treiber auf dem Server zu filtern.
   - Klicken Sie auf das Symbol , um alle Treiber zu filtern, die gestartet werden.
   - Klicken Sie auf das Symbol , um alle Treiber zu filtern, die gestoppt werden.
   - Klicken Sie auf das Symbol , um die Treiber herauszufiltern, denen kein Status zugeordnet ist. Wenn ein Treibersatz mit keinem Server verknüpft ist, wird für die in diesem Treibersatz enthaltenen Treiber der Status **Unbekannt** angezeigt.

   Um alle Filter zu löschen, die für die Treiber angewendet wurden, klicken Sie auf das Symbol , das auf der Kachel zum **Treiberstatus** angezeigt wird.
3. Die Treibersätze können auch über das Identity Console-Portal gefiltert werden. Standardmäßig werden im Identity Console-Portal alle Treiber angezeigt, die mit einem beliebigen Treibersatz auf Ihrem Server verknüpft sind. Wenn Sie die Treiber eines bestimmten Treibersatzes anzeigen möchten, müssen Sie den gewünschten Treibersatz aus der Liste der Treibersätze auf der linken Seite im Identity Console-Portal auswählen. Um die Treibersatzauswahl aufzuheben, klicken Sie erneut auf den ausgewählten Treibersatz.

Abbildung 21-6 *Treiber und Treibersätze filtern*

Treibersatz löschen

Führen Sie die folgenden Schritte aus, um einen Treibersatz zu löschen:

1. Klicken Sie auf dem Identity Console-Startbildschirm auf die Registerkarte **IDM-Administration**.
2. Klicken Sie auf die Aktionsschaltfläche ⋮ im entsprechenden Treibersatz, den Sie löschen möchten.
3. Klicken Sie auf **Löschen**.

Treiberaktionen

Die folgenden Aktionen werden beim Klicken auf das Aktionssymbol ⋮ auf der Kachel des einzelnen Treibers unterstützt:

- **Treiber starten**: Einen Treiber starten.
- **Treiber stoppen**: Einen Treiber stoppen.
- **Treiber neu starten**: Einen gestoppten Treiber neu starten.
- **Treiber löschen**: Einen Treiber löschen.
- **Statistik**: Leistungsstatistik des Treibers anzeigen.
- **Daten kopieren**: Treiberdaten von einem Server zu einem anderen Server kopieren. Diese Option ist nur für eine Umgebung mit mehreren Servern verfügbar.

22 Treibersatzeigenschaften verwalten

Dieser Abschnitt enthält Informationen zu den allgemeinen Eigenschaften eines Treibersatzes. Dies umfasst alle Eigenschaften (benanntes Passwort, Protokollierumfang, Treibersatzinspektor usw.).

Dieser Abschnitt behandelt die folgenden Themen:

Treibersätze konfigurieren

Führen Sie die folgenden Schritte aus, um die Konfiguration eines Treibersatzes zu ändern:

1. Klicken Sie auf **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften**.
2. Standardmäßig wird die Seite **Treibersatzkonfiguration** angezeigt. Die Optionen für die Treibersatzkonfiguration sind in die folgenden Kategorien unterteilt:

Benanntes Passwort

Mit Identity Manager können Sie mehrere Passwörter für einen Treibersatz sicher speichern. Diese Funktionalität wird als „Benannte Passwörter“ bezeichnet. Der Zugriff auf die einzelnen Passwörter erfolgt über einen Schlüssel bzw. Namen.

Sie können benannte Passwörter zu einem Treibersatz oder zu einzelnen Treibern hinzufügen. Benannte Passwörter für einen Treibersatz sind für alle Treiber im Satz verfügbar.

Wenn Sie ein benanntes Passwort in einer Treiberrichtlinie verwenden möchten, verweisen Sie mit dem Namen des Passworts darauf, anstatt das eigentliche Passwort zu verwenden. Das Passwort wird dann über die Identity Manager-Engine an den Treiber gesendet. Die in diesem Abschnitt beschriebene Methode zum Speichern und Abrufen von benannten Passwörtern kann für alle Treiber verwendet werden, ohne dass Änderungen am Treiber-Shim erforderlich sind.

Der Zugriff auf benannte Passwörter erfolgt über **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Benanntes Passwort** unter **Treibersatzkonfiguration**.

Um ein neues benanntes Passwort hinzuzufügen, klicken Sie auf das Symbol +. Um ein vorhandenes benanntes Passwort zu entfernen, wählen Sie das jeweilige Passwort aus und klicken Sie auf das Symbol .

Globalkonfigurationswerte

Zeigt eine geordnete Liste der Objekte der globalen Konfiguration an. Die Objekte enthalten Definitionen für globale Konfigurationswerte für den Treiber in einer GCV-Datei, die Identity Manager beim Starten des Treibers lädt. Sie können die Objekte der globalen Konfiguration hinzufügen oder entfernen und die Reihenfolge ändern, in der die Objekte ausgeführt werden.

Klicken Sie auf das Symbol , um die globalen Konfigurationswerte zu speichern. Um die Liste der globalen Konfigurationswerte zu aktualisieren, klicken Sie auf das Symbol .

Java-Umgebungsparameter konfigurieren

Führen Sie die folgenden Schritte aus, um Java-Umgebungsparameter zu konfigurieren:

1. Wählen Sie in Identity Console **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** aus.
2. Klicken Sie auf **Java-Umgebungsparameter** unter **Treibersatzkonfiguration**, um die Eigenschaftsseite mit den Java-Umgebungsparametern anzuzeigen.
3. Bearbeiten Sie die folgenden Einstellungen je nach Bedarf:

   Hinzufügungen zum Klassenpfad: Geben Sie zusätzliche Pfade an, in denen die JVM nach Paket- (`.jar`) und Klassendateien (`.class`) suchen soll. Die Verwendung dieses Parameters entspricht der Verwendung des Befehls `java -classpath`. Wenn Sie mehrere Klassenpfade eingeben, trennen Sie diese bei einer Windows-JVM durch ein Semikolon (;) und bei einer UNIX- oder Linux-JVM durch einen Doppelpunkt (:).

   JVM-Optionen: Geben Sie weitere Optionen an, die mit der JVM verwendet werden sollen. Weitere Informationen über gültige Optionen finden Sie in der JVM-Dokumentation.

   Die entsprechende Umgebungsvariable ist `DHOST_JVM_OPTIONS`. Sie gibt die Argumente für JVM 1.2 an. Beispiel:

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Jede Optionszeichenkette ist durch Leerzeichen getrennt. Wenn eine Optionszeichenkette Leerzeichen enthält, muss sie in doppelte Anführungszeichen gesetzt werden.

   Die Treibersatz-Attributoption hat Vorrang vor der Umgebungsvariable `DHOST_JVM_OPTIONS`. Diese Umgebungsvariable wird an das Ende der Option zum Festlegen der Attribute im Treiber angehängt.

   Ausgangs-Heap-Größe: Geben Sie die anfängliche Mindest-Heap-Größe an, die der JVM zur Verfügung steht. Durch das Erhöhen der Ausgangs-Heap-Größe können die Startzeit und die Durchsatzleistung verbessert werden. Verwenden Sie einen numerischen Wert gefolgt von G, M oder K. Wenn kein Buchstabe angegeben wird, wird die Größe standardmäßig auf Bytes festgelegt. Die Verwendung dieses Parameters entspricht der Verwendung des Befehls `java -Xms`.

Die entsprechende Umgebungsvariable ist DHOST_JVM_INITIAL_HEAP. Sie gibt die anfängliche JVM-Heap-Größe in Dezimalschreibweise in Bytes an. Sie hat Vorrang vor der Treibersatz-Attributoption.

Informationen über die anfängliche Standard-Heap-Größe der JVM finden Sie in der JVM-Dokumentation.

Maximale Heap-Größe: Geben Sie die maximale Heap-Größe an, die der JVM zur Verfügung steht. Verwenden Sie einen numerischen Wert gefolgt von G, M oder K. Wenn kein Buchstabe angegeben wird, wird die Größe standardmäßig auf Bytes festgelegt. Die Verwendung dieses Parameters entspricht der Verwendung des Befehls `java -Xmx`.

Die entsprechende Umgebungsvariable ist DHOST_JVM_MAX_HEAP. Gibt die maximale JVM-Heap-Größe in Dezimalschreibweise in Bytes an. Sie hat Vorrang vor der Treibersatz-Attributoption.

Informationen über die maximale Standard-Heap-Größe der JVM finden Sie in der JVM-Dokumentation.

4 Klicken Sie zum Speichern der Änderungen auf .

5 Starten Sie das Identitätsdepot neu, um die Änderungen anzuwenden.

Liste der Attribute mit Wert verwalten

Führen Sie die folgenden Schritte aus, um für einen bestimmten Treibersatz Attribute zur Liste der Attribute mit Wert hinzuzufügen:

1 Wählen Sie in Identity Console das Modul **Objektverwaltung** aus.

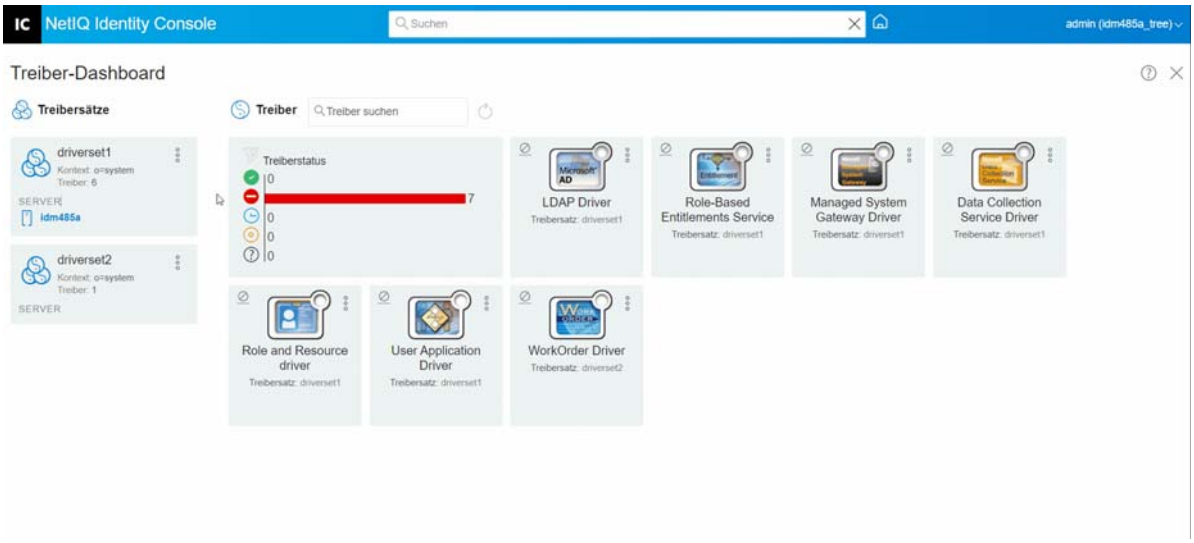
2 Wählen Sie den Typ **DirXML-DriverSet** (DirXML-Treibersatz) aus der Dropdown-Liste aus und klicken Sie auf die Suchschaltfläche.

3 Klicken Sie in der Suchliste auf den entsprechenden Treibersatz.

4 Um Attribute ohne Wert zur Liste der Attribute mit Wert hinzuzufügen, klicken Sie auf das Symbol + neben **Attribute mit Wert** und wählen Sie die entsprechenden Attribute ohne Wert aus der Liste aus.

5 Wenn Sie fertig sind, klicken Sie auf **OK**.

Abbildung 22-1 *Konfigurationsparameter für Treibersätze verwalten*



Aufträge für Treibersätze verwalten

Mit Identity Console können Sie mit der Option „Aufträge“ Ereignisse für alle Treiber planen, die sich im jeweiligen Treibersatz befinden.

Die Seite „Job Scheduler“ (Auftragsplaner) enthält den Auftragsnamen, die Angabe, ob ein Auftrag aktiviert oder deaktiviert ist, zu welchem Zeitpunkt er ausgeführt werden soll sowie die Auftragsbeschreibung. Klicken Sie auf den Auftragsnamen, um die Seite „Aufträge“ aufzurufen. Klicken Sie in der Spalte „Aktiviert“ auf das Symbol zum Aktivieren/Deaktivieren, um den Auftrag zu aktivieren bzw. zu deaktivieren. Klicken Sie auf die Auftragsbeschreibung, um die vollständige Beschreibung des Auftrags anzuzeigen.

Der Zugriff auf die Seite „Aufträge“ erfolgt durch Klicken auf **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > Registerkarte **Erweitert** auf der Identity Console-Hauptseite. Die Registerkarte „Aufträge“ enthält eine Tabelle mit den vorhandenen Auftragsobjekten für den ausgewählten Treiber, der mit dem vollständigen eindeutigen Namen (DN) im Treibereintrag aufgelistet wird.

Auf der Seite „Job Scheduler“ (Auftragsplaner) können Sie die folgenden Aufgaben ausführen:

- **Auftrag erstellen**: Klicken Sie auf das Symbol +, um einen neuen Auftrag zu erstellen.

  Führen Sie im Popup-Fenster **Neuer Auftrag** die folgenden Schritte aus, um einen neuen Auftrag zu erstellen:

  1. Geben Sie den Auftragsnamen an.
  2. Wählen Sie den Auftragstyp aus.
  3. Klicken Sie auf das Symbol ∨ und wählen Sie in der Liste der verfügbaren Server den Server aus, auf dem Sie den Auftrag ausführen möchten. Geben Sie andernfalls einen Servernamen an und wählen Sie dann den Server aus.
  4. Klicken Sie auf die Schaltfläche **Erstellen**.

- **Auftrag starten**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .
- **Auftrag stoppen**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .
- **Auftrag aktivieren**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .
- **Auftrag deaktivieren**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .
- **Zustand abrufen**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .
- **Auftrag löschen**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .

Klicken Sie auf einen Auftrag, um die Seite **Auftragseigenschaften** aufzurufen. Hier können Sie festlegen, wie der Auftrag ausgeführt werden soll.

Allgemein: Zeigt den Java-Klassennamen für den Auftrag an. Auf dieser Seite können Sie einen Auftrag aktivieren oder deaktivieren, den Auftrag nach seiner Ausführung löschen, die Server auswählen, auf denen der Auftrag ausgeführt werden soll, den Email-Server angeben, einen anderen Anzeigenamen und eine andere Beschreibung für den Auftrag eingeben.

Zeitplan: Hier können Sie festlegen, wann der Auftrag ausgeführt werden soll. Geben Sie unter „Auftrag starten um“ die gewünschte Startuhrzeit an und legen Sie fest, ob der Auftrag täglich, wöchentlich, monatlich oder jährlich ausgeführt werden soll. Sie können auch benutzerdefiniert anpassen, wann Sie den Auftrag ausführen möchten, oder Sie können den Umschalter aktivieren, um den Auftrag manuell auszuführen.

Bereich: Mit dieser Option können Sie die Objekte definieren, für die dieser Auftrag gilt. Ein Objekt kann ein Container, eine dynamische Gruppe, eine Gruppe oder ein Blattobjekt sein. Klicken Sie auf "Hinzufügen", um ein Objekt auszuwählen, für das dieser Auftrag gilt. Wählen Sie ein Objekt aus, indem Sie auf die Schaltfläche "Durchsuchen" und anschließend auf "OK" klicken. Wählen Sie zum Entfernen einen Objekts aus der Liste "Bereich" das entsprechende Bereichsobjekt aus, indem Sie das Feld links neben dem DN-Objekt aktivieren und anschließend auf "Entfernen" klicken.

Wählen Sie ein hinzugefügtes Objekt aus, um weitere Optionen anzuzeigen. Bei Auswahl eines Gruppenobjekts können Sie den Auftrag entweder auf die Gruppenmitglieder oder nur auf die Gruppe anwenden. Bei Auswahl eines Containerobjekts können Sie den Auftrag auf alle nachgeordneten Einheiten im Container, auf alle untergeordneten Elemente im Container oder nur auf den Container anwenden.

Parameter: Mit dieser Option können Sie dem Auftrag zusätzliche Parameter hinzufügen und die zurzeit eingerichteten Parameter anzeigen. Je nach ausgewähltem Auftrag können sich diese Parameter ändern.

Ergebnisse: Mit dieser Option können Sie definieren, wie die Ergebnisse des Auftrags verarbeitet werden sollen. Die Seite "Ergebnisse" besteht aus zwei Teilen: "Zwischenergebnis" und "Endergebnis". Folgende Ergebnisse sind zulässig: "Erfolg", "Warnhinweis", "Fehler" und "Abgebrochen". Rechts neben der Spalte "Ergebnisse" befindet sich die Spalte "Aktion". Wenn Sie auf die Spalte "Aktion" klicken, können Sie den Benachrichtigungstyp für die einzelnen Ergebnisse

festlegen. Zu den Aktionen gehören z. B. das Versenden eines Audit-Ergebnisses oder das Versenden einer Email nach Fertigstellung der Aufgabe. Wenn Sie keine Option auswählen, wird für das entsprechende Ergebnis keine Aktion vorgenommen.

Auf der Registerkarte **Trace** können Sie ein Trace für einen bestimmten Treiber konfigurieren. Weitere Informationen finden Sie unter „Trace-Stufe konfigurieren“, auf Seite 175.

Bibliotheken für einen spezifischen Treibersatz verwalten

Bibliotheksobjekte speichern mehrere Richtlinien und andere Ressourcen, die von einem oder mehreren Treibern gemeinsam genutzt werden. Ein Bibliotheksobjekt kann in einem Treibersatzobjekt oder einem beliebigen eDirectory-Container erstellt werden. In einem eDirectory-Baum können mehrere Bibliotheken vorhanden sein. Treiber können auf jede Bibliothek im Baum verweisen, solange der Server, auf dem der Treiber ausgeführt wird, ein Lese-/Schreib- oder Masterreplikat des Bibliotheksobjekts enthält.

Formatvorlagen, Richtlinien, Regeln und andere Ressourcenobjekte können in einer Bibliothek gespeichert und von einem oder mehreren Treibern referenziert werden.

Mit dem Bibliotheksverwaltungsmodul können Sie die folgenden Aufgaben ausführen:

- „Vorhandene Bibliotheken anzeigen und löschen“, auf Seite 146
- „Objekte der Bibliothek anzeigen oder löschen“, auf Seite 146

Vorhandene Bibliotheken anzeigen und löschen

Führen Sie die folgenden Schritte aus, um eine vorhandene Bibliothek anzuzeigen oder zu löschen:

1. Klicken Sie in Identity Console auf **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Erweitert** > **Bibliotheken**.
2. Wählen Sie die entsprechende Bibliothek aus der Liste aus.
3. Klicken Sie auf das Symbol  . Klicken Sie zur Bestätigung auf **OK**.

Objekte der Bibliothek anzeigen oder löschen

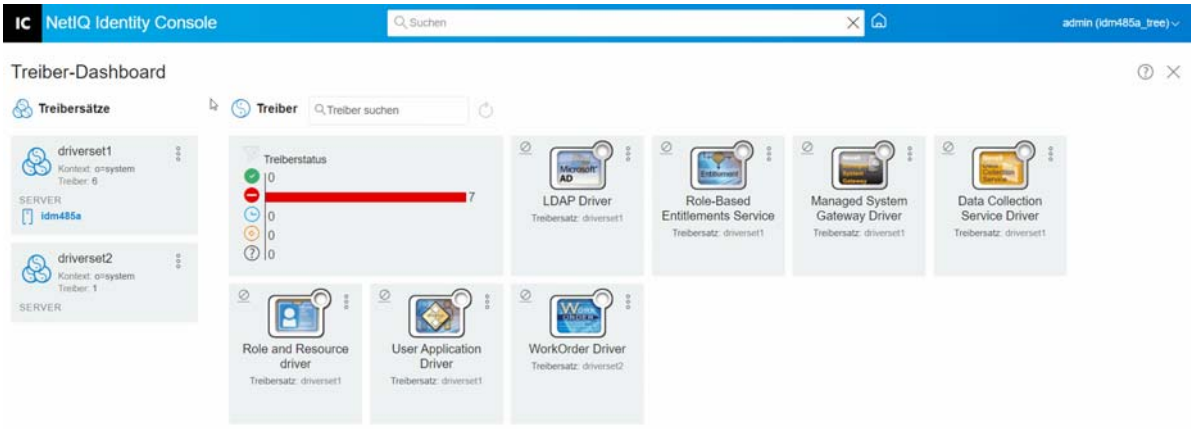
Sie können Richtlinien und Zuordnungstabellen aus Bibliotheksobjekten anzeigen und löschen. Führen Sie die folgenden Schritte aus, um Objekte zu löschen:

1. Klicken Sie in Identity Console auf **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Erweitert** > **Bibliotheken**.
2. Klicken Sie in der Liste auf die entsprechende Bibliothek.
3. Um Richtlinien zu löschen, wählen Sie die Registerkarte **Richtlinien** aus.
4. Wählen Sie die entsprechende Richtlinie aus der Liste aus und klicken Sie auf das Symbol  .
5. Um Zuordnungstabellen zu löschen, wählen Sie die Registerkarte **Zuordnungstabellen** aus.

6 Wählen Sie die entsprechende Zuordnungstabelle aus der Liste aus und klicken Sie auf das Symbol .

7 Klicken Sie zur Bestätigung auf **OK**.

Abbildung 22-2 *Aufträge und Bibliotheken für Treibersätze verwalten*



Protokollierumfang und Trace-Stufe von Treibersätzen konfigurieren

Um den Protokollierumfang und die Trace-Stufe für Ihre Treibersätze zu konfigurieren, wählen Sie auf der Identity Console-Hauptseite **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Protokoll- und Trace-Konfiguration** aus. Dieser Abschnitt behandelt die folgenden Themen:

- „Protokollierumfang konfigurieren“, auf Seite 147
- „Trace-Stufe konfigurieren“, auf Seite 148
- „DirXML-Skript-Tracing“, auf Seite 149

Protokollierumfang konfigurieren

Jeder Treibersatz hat ein Feld „Protokollierumfang“, über das Sie festlegen können, in welchem Umfang Fehler protokolliert werden sollen. Die hier angegebene Stufe bestimmt, welche Meldungen in den Protokollen verfügbar sind. Standardmäßig ist der Protokollierumfang auf Fehlermeldungen eingeschränkt (dazu gehören auch schwerwiegende Fehler). Um zusätzliche Nachrichtentypen nachzuverfolgen, ändern Sie den Protokollierumfang. Um den Protokollierumfang zu konfigurieren, wählen Sie In Identity Console **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Protokoll- und Trace-Konfiguration** > **Protokollierumfang** aus. Die folgende Tabelle beschreibt die Einstellungen für den Protokollierumfang:

Option	Beschreibung
Protokollierung in Treibersatz-, Abonnenten- und Herausgeberprotokollen deaktivieren	Deaktiviert die gesamte Protokollierung für alle Treiber im Treibersatzobjekt, im Abonnentenkanal und im Herausgeberkanal.
Höchstanzahl an Einträgen im Protokoll (50–500)	Anzahl der Einträge im Protokoll. Der Standardwert ist 50.
Protokollierumfang	Die folgenden Einstellungen stehen für den Protokollierumfang zur Auswahl: ◆ **Fehler protokollieren**: Nur Fehler werden protokolliert. ◆ Fehler und Warnungen protokollieren: Fehler und Warnmeldungen werden protokolliert. ◆ **Spezifische Ereignisse protokollieren**: Die ausgewählten Ereignisse werden protokolliert. Wenn Sie diese Option auswählen, wird die folgende Liste von Ereignissen aktiviert: ◆ **Metadirectory-Engine-Ereignisse** ◆ **Statusereignisse** ◆ **Vorgangsereignisse** ◆ **Transformationsereignisse** ◆ **Berechtigungsbereitstellungsereignisse** ◆ **Nur letzte Protokollierungszeit aktualisieren**: Die letzte Protokollierungszeit wird aktualisiert. ◆ **Protokollierung deaktiviert**: Die Protokollierung wird für den Treiber deaktiviert.

Trace-Stufe konfigurieren

Sie können die Trace-Stufe für einen bestimmten Treibersatz konfigurieren. Je nach der für einen bestimmten Treibersatz festgelegten Trace-Stufe werden im Trace treiberbezogene Ereignisse angezeigt, wenn die Engine die Ereignisse verarbeitet. Die Treiber-Trace-Stufe gilt nur für den Treiber oder Treibersatz, für den das Trace festgelegt ist. Wenn Sie Remote Loader verwenden, wird die Remote Loader-Trace-Datei direkt auf Remote Loader festgelegt und enthält nur das Treiber-Shim-Trace.

Um die Trace-Stufe für einen Treibersatz zu konfigurieren, wählen Sie **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Protokoll- und Trace-Konfiguration** > Registerkarte **Trace** aus. Die folgende Tabelle beschreibt die Trace-Einstellungen:

Parameter	Treiber
Trace-Stufe	Je höher die Treiber-Trace-Stufe, desto mehr Informationen werden im Trace angezeigt. Trace-Stufe 1 zeigt Fehler, aber nicht die Ursache für die Fehler an. Wenn Sie Informationen zur Passwortsynchronisierung anzeigen möchten, setzen Sie die Trace-Stufe auf 5. Wenn Sie **Einstellungen aus dem Treibersatz verwenden** auswählen, wird der Wert vom Treibersatz übernommen.
XSL-Trace-Stufe	Trace zeigt XSL-Ereignisse an. Verwenden Sie diese Trace-Stufe nur bei der Fehlerbehebung in XSL-Formatvorlagen. Wenn keine XSL-Informationen angezeigt werden sollen, setzen Sie die Stufe auf 0.
Port für die Java-Fehlersuche	Ermöglicht Entwicklern den Einsatz eines Java-Fehlersuchprogramms (Debugger). Starten Sie das Identitätsdepot neu, nachdem Sie das Java-Fehlersuchprogramm angefügt haben.
Trace-Datei	Geben Sie den Namen und Speicherort einer Datei an, in die die Identity Manager-Informationen für den ausgewählten Treiber geschrieben werden. Wenn Sie **Einstellungen aus dem Treibersatz verwenden** auswählen, wird der Wert vom Treibersatz übernommen.
Kodierung der Trace-Datei	Die Trace-Datei verwendet die Standardkodierung des Systems. Sie können bei Bedarf eine andere Kodierung angeben. Wenn Sie **Einstellungen aus dem Treibersatz verwenden** auswählen, wird der Wert vom Treibersatz übernommen.
Größenlimit der Trace-Datei	Ermöglicht Ihnen das Festlegen eines Größenlimits für die Java-Trace-Datei. Wenn Sie die Dateigröße auf „Unbegrenzt“ setzen, nimmt die Datei so lange an Größe zu, bis kein Festplattenplatz mehr vorhanden ist. **HINWEIS:** Wenn eine Dateigrößenbeschränkung angegeben wird, wird die Trace-Datei in mehreren Dateien erstellt. Identity Manager teilt automatisch die maximale Dateigröße durch zehn und erstellt zehn separate Dateien. Die kombinierte Größe dieser Dateien entspricht der maximalen Größe der Trace-Datei. Wenn Sie **Einstellungen aus dem Treibersatz verwenden** auswählen, wird der Wert vom Treibersatz übernommen.

DirXML-Skript-Tracing

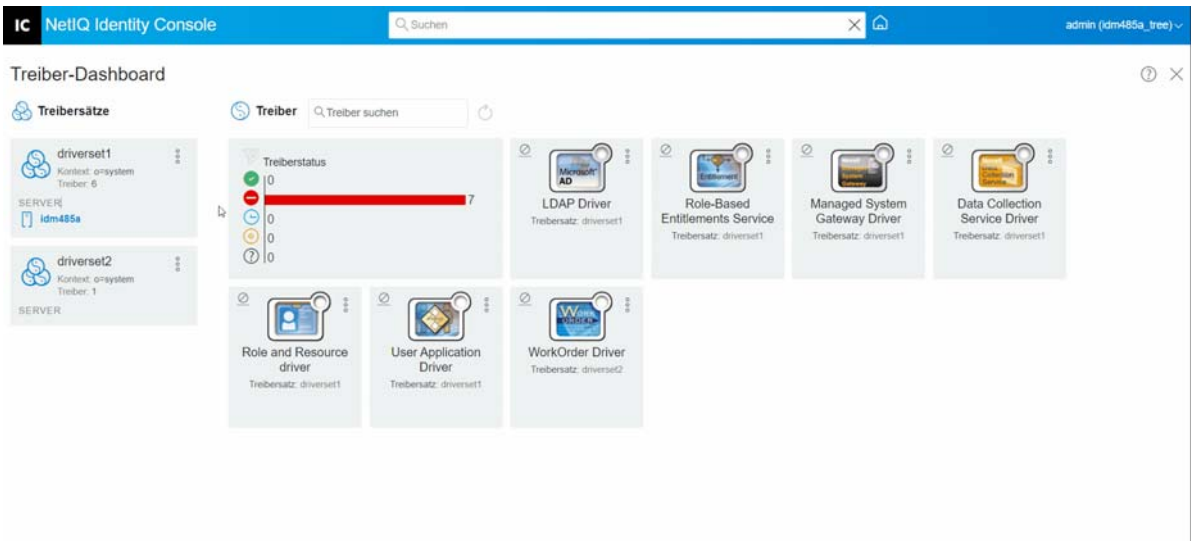
Mit der Option des DirXML-Skript-Tracing können Sie eine Trace-Stufe für einen Treibersatz auswählen. Die Auswahl wird auf alle Richtlinien im Treibersatz angewendet. Für das DirXML-Skript-Tracing stehen die folgenden Optionen zur Auswahl:

- Gesamtes DirXML-Skript-Tracing aktiviert
- Gesamtes DirXML-Skript-Tracing deaktiviert

- DirXML-Skriptregel-Tracing aktiviert
- DirXML-Skriptregel-Tracing deaktiviert

Klicken Sie zum Speichern der Änderungen auf .

Abbildung 22-3 *Protokollierumfang und Trace-Stufe von Treibersätzen verwalten*



Treibersatzinspektor und Statistik verwalten

Mit dem Treibersatzinspektor können Sie detaillierte Informationen zu den Objekten anzeigen, die mit einem Treibersatz verknüpft sind. Dieser Abschnitt behandelt die folgenden Themen:

- „Treibersatzstatistiken anzeigen“, auf Seite 150
- „Anzeigen der Versionsinformationen“, auf Seite 151
- „Verknüpfungsstatistik anzeigen“, auf Seite 152

Treibersatzstatistiken anzeigen

Im Identity Console-Portal können Sie eine Vielzahl von Statistiken für einen einzelnen Treiber oder für einen gesamten Treibersatz anzeigen. Dazu gehören Statistiken wie die Cache-Dateigröße, die Größe der nicht verarbeiteten Transaktionen in der Cache-Datei, die älteste und neueste Transaktion sowie die Gesamtzahl der nicht verarbeiteten Transaktionen nach Kategorie (Hinzufügungen, Entfernungen, Änderungen usw.). So zeigen Sie die Treibersatzstatistiken an:

1 Wählen Sie in Identity Console **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Inspektor und Statistik** > **Statistik** aus.

2 Wählen Sie in der Dropdown-Liste den gewünschten Server aus.

Eine Seite wird angezeigt, auf der Sie die Statistik für alle im Treibersatz enthaltenen Treiber anzeigen können.

- Um die Statistik zu aktualisieren, klicken Sie auf das Symbol .

- Um die Statistik für einen Treiber zu schließen, klicken Sie auf die Schaltfläche  in der oberen rechten Ecke des Statistikfensters des Treibers.
- Um die Statistik für alle Treiber zu öffnen, klicken Sie auf **Aktionen** > **Alle anzeigen**.
- Um die Liste der nicht verarbeiteten Transaktionen für einen Treiber zu reduzieren, klicken Sie auf die Schaltfläche oberhalb der Liste. Um die Liste der nicht verarbeiteten Transaktionen für alle Treiber zu reduzieren, klicken Sie auf die Schaltfläche **Aktionen** > **Alle Transaktionen reduzieren**.
- Um die Liste der Transaktionen zu erweitern, klicken Sie auf die Schaltfläche . Um die Liste der nicht verarbeiteten Transaktionen für alle Treiber zu erweitern, klicken Sie auf **Aktionen** > **Alle Transaktionen erweitern**.
- Um das Statistik-Dashboard für deaktivierte Treiber zu schließen, klicken Sie auf **Aktionen** und wählen Sie dann **Deaktivierte Treiber ausblenden** aus.

Anzeigen der Versionsinformationen

Die Identity Manager-Engine, die Treiber-Shims und die Treiberkonfigurationsdateien enthalten jeweils eine separate Versionsnummer. Mit der Option „Versionsermittlung“ in Identity Console können Sie die Versionen der Identity Manager-Engine und der Treiber-Shims ermitteln. Die Treiberkonfigurationsdateien enthalten ihre eigene Namenskonvention. So zeigen Sie die Versionsinformationen an:

1. Wählen Sie in Identity Console **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Inspektor und Statistik** > **Versionsermittlung** aus.
2. Versionsinformationen in der Übersicht anzeigen:
   - Die eDirectory-Baumstruktur, für die Sie authentifiziert sind

     HINWEIS: In der Identity Manager-Umgebung wird eDirectory als Identitätsdepot bezeichnet.
   - Der Treibersatz, den Sie ausgewählt haben
   - Die Server, die dem Treibersatz zugeordnet sind

     Wenn der Treibersatz zwei oder mehreren Servern zugeordnet ist, können Sie die Identity Manager-Informationen auf jedem Server anzeigen.
   - Treiber
3. Klicken Sie auf das Symbol **Anzeigen**  , um eine Textdarstellung der Informationen aus der Übersicht anzuzeigen.
4. Klicken Sie auf die Schaltfläche „Exportieren“  , um den Text in eine Datei zu exportieren und auf dem lokalen Laufwerk oder auf einem Netzlaufwerk zu speichern.

Verknüpfungsstatistik anzeigen

Die Identity Manager-Funktion „Verknüpfungsstatistik“ zeigt die Verknüpfungsdetails der mit Identity Manager verwalteten Identitäten. Anhand der Verknüpfungsstatistik ermittelt Identity Manager die Anzahl der Verknüpfungen für die Identity Manager-Treiber.

Führen Sie den Verknüpfungsstatistikauftrag aus, um aktive, inaktive und systemverwaltete Objekte für einen Treiber abzurufen. Sie können den Verknüpfungsstatistikauftrag zur täglichen, wöchentlichen, monatlichen oder jährlichen Ausführung planen. Standardmäßig ist der Auftrag zur wöchentlichen Ausführung geplant.

Im Verknüpfungsstatistik-Dashboard werden die Verknüpfungsdetails angezeigt. Alternativ können Sie die Verknüpfungen in eine Datei exportieren, um die Details anzuzeigen.

HINWEIS

- Die Verknüpfungsanzahl für die Treiber wird pro Server angegeben. Wenn ein Objekt mit mehr als einem Treiber verknüpft ist, wird die Verknüpfungsanzahl für jeden Treiber eindeutig berechnet.
- Wenn Sie mehr als 200.000 Verknüpfungen haben, empfiehlt es sich, die maximale Heap-Größe für den Treibersatz auf 2 GB oder mehr festzulegen. Informationen zum Festlegen der Heap-Größe finden Sie unter „Java-Umgebungsparameter konfigurieren“, auf Seite 142.

So zeigen Sie die Verknüpfungsstatistik an:

1. Wählen Sie in Identity Console **IDM-Administration** > **Kontextmenü (drei Punkte) des entsprechenden Treibersatzes** > **Treibersatzeigenschaften** > **Inspektor und Statistik** > **Verknüpfungsstatistik** aus.
2. Wählen Sie den Server aus, für den Sie die Verknüpfungsstatistik ausführen möchten.
3. Die Verknüpfungsanzahl zeigt das zuvor berechnete Ergebnis an.

   Identity Console zeigt die Verknüpfungsanzahl für aktive, inaktive und systemverwaltete Objekte für alle mit dem Treibersatz verknüpften Treiber an.

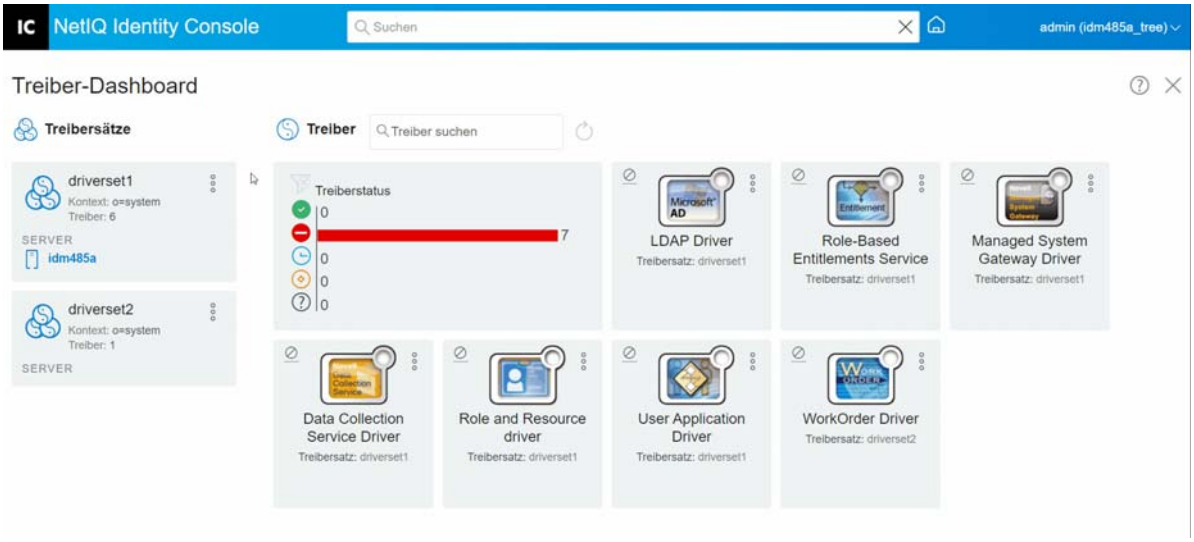
   Identity Console betrachtet Gruppen und Organisationseinheiten als systemverwaltete Objekte. Identity Console betrachtet ein Objekt als inaktiv, wenn das Attribut `Anmeldung deaktiviert` im Objekt auf „true“ (wahr) festgelegt ist und das Objekt innerhalb der letzten 120 Tage nicht geändert wurde. Alle übrigen Objekte werden als aktive verwaltete Objekte betrachtet.
4. Klicken Sie auf das Symbol , um die aktualisierten Ergebnisse zu erhalten.

   Wenn ein Treiber auf dem Server deaktiviert ist, zeigt Identity Console den Treiber nicht im Dashboard an.
5. Klicken Sie auf das Symbol , um die Systemdetails und Details zur Verknüpfungsanzahl für die mit dem Server verknüpften Treiber zu exportieren.
6. Um die Objekte zu exportieren, die mit einem bestimmten Treiber verknüpft sind, klicken Sie neben den erforderlichen Objekten auf und speichern Sie die Datei.

HINWEIS: Bei Auffächerungstreibern werden nur eindeutige Objekte exportiert. Wenn ein Objekt mit mehreren Instanzen eines Auffächerungstreibers verknüpft ist, zeigt Identity Console alle Verknüpfungsanzahlen im Dashboard an. Wenn Sie jedoch die Objekte in einer Datei exportieren, exportiert Identity Console nur die eindeutigen Objekte.

7 Klicken Sie auf **Aktionen** und wählen Sie die erforderliche Option aus, um das Verknüpfungsanzahl-Dashboard zu organisieren.

Abbildung 22-4 *Treibersatzstatistiken verwalten*



23 Treibereigenschaften verwalten

Dieser Abschnitt enthält Informationen zu den allgemeinen Eigenschaften eines Treibers. Dies umfasst alle Eigenschaften (benanntes Passwort, Engine-Steuerelementwerte, Protokollierumfang usw.).

Die Aktivierungsinformationen für einen Treiber werden angezeigt und erinnern Sie an die Aktion zum Aktivieren des ablaufenden Treibers.

Führen Sie die folgenden Schritte aus, um die Konfiguration des Treibers zu ändern:

1. Klicken Sie auf dem Identity Console-Startbildschirm auf die Registerkarte **Treiber**.
2. Klicken Sie auf die Kachel des entsprechenden Treibers, um die Konfigurationsseite des Treibers anzuzeigen.

   Standardmäßig wird die Seite **Verbindungsparameter** angezeigt. Die Optionen für die Treiberkonfiguration sind in die folgenden Kategorien unterteilt:

Verbindungsparameter

Die Verbindungsparameter steuern, ob der Treiber lokal oder remote ausgeführt werden soll.

- **Java:** Geben Sie mit dieser Option den Namen der Java-Klasse an, die für das Treiber-Shim instanziiert wird. Diese Klasse kann sich als Klassendatei im Klassenverzeichnis oder als JAR-Datei im Verzeichnis `lib` befinden. Wählen Sie diese Option aus, um den Treiber lokal auszuführen. Sie müssen auch das Treiberobjektpasswort und das Treiber-Cache-Limit angeben. Sie können ein neues Passwort festlegen, indem Sie auf den Link **Passwort festlegen** klicken.

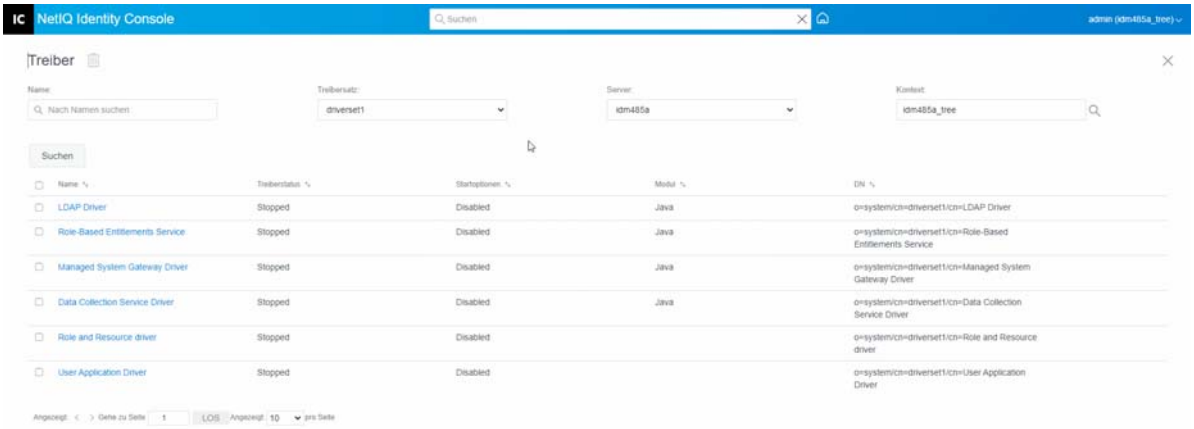
  Beispiel: `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`
- **Native:** Unter dieser Option wird der Name der in nativer Programmiersprache (wie C++) entwickelten `.dll` für den Treiber angegeben. Sie müssen auch das Treiberobjektpasswort und das Treiber-Cache-Limit angeben. Sie können ein neues Passwort festlegen, indem Sie auf den Link **Passwort festlegen** klicken.

  Beispiel: `addriver.dll`

- **Mit Remote Loader verbinden:** Diese Option wird verwendet, wenn der Treiber eine Remoteverbindung zum verbundenen System herstellt. Wenn diese Option aktiviert ist, müssen Sie die folgenden Unteroptionen angeben:
  - **Remote Loader-Verbindungsparameter**: Dies enthält Details zur Remote Loader-Umgebung wie Hostname, Verbindungsport usw.
  - **Remote Loader-Passwort**: Das Passwort für Remote Loader.
  - **Treiberobjektpasswort**: Legt ein Passwort für das Treiberobjekt fest. Wenn Sie Remote Loader verwenden, müssen Sie auf dieser Seite ein Passwort eingeben. Remote Loader verwendet dieses Passwort zur Authentifizierung beim Remote-Treiber-Shim.
- **Authentifizierung**: Die Authentifizierungsparameter werden für die Authentifizierung der Identity Manager-Engine und der Remote Loader-Server verwendet. Geben Sie die folgenden Parameter an:
  - **Authentifizierungs-ID**: Geben Sie eine Benutzeranwendungs-ID an. Anhand dieser ID werden die Abonnementinformationen vom Identitätsdepot an die Anwendung übergeben.
  - **Authentifizierungskontext**: Geben Sie die IP-Adresse oder den Namen des Servers ein, mit dem das Anwendungs-Shim kommunizieren soll.
  - **Anwendungspasswort**: Option zum Festlegen des Anwendungsauthentifizierungspassworts.

Wenn Sie fertig sind, klicken Sie auf das Symbol , um die Konfiguration zu speichern.

Abbildung 23-1 *Verbindungsparameter verwalten*



Treiberkonfiguration

Im Treiberkonfigurationsbereich können Sie die treiberspezifischen Parameter, Engine-Steuerelementwerte, globalen Konfigurationswerte usw. konfigurieren. Durch Ändern der Treiberparameter können Sie das Treiberverhalten auf Ihre Netzwerkumgebung abstimmen. Dieser Abschnitt behandelt die folgenden Themen:

Treiberparameter

Die Treiberparameter sind in Treibereinstellungen, Abonnenteneinstellungen und Herausgebereinstellungen unterteilt. Diese Einstellungen werden basierend auf der Treiberkonfiguration aufgefüllt. Weitere Informationen zu den Treiberparametern finden Sie im spezifischen Treiberhandbuch in der Dokumentation Identity Manager Drivers (Identity Manager-Treiber).

Wenn Sie fertig sind, können Sie die Parameter durch Klicken auf  speichern. Wenn Sie die Parameter auf den Standardwert festlegen möchten, klicken Sie auf das Symbol  . Um die Treiberkonfiguration mithilfe der XML-Datei zu ändern, klicken Sie auf das Symbol  .

Globalkonfigurationswerte

Zeigt eine geordnete Liste der Objekte der globalen Konfiguration an. Die Objekte enthalten Definitionen für globale Konfigurationswerte für den Treiber in einer GCV-Datei, die Identity Manager beim Starten des Treibers lädt. Sie können die Objekte unter der Registerkarte **Globale Konfigurationswerte** mit dem XML-Editor anzeigen oder ändern. Klicken Sie auf das Symbol  , um die globalen Konfigurationswerte zu speichern. Um die Liste der globalen Konfigurationswerte zu aktualisieren, klicken Sie auf das Symbol  . Um globale Konfigurationswerte zu löschen, wählen Sie das entsprechende globale Konfigurationswerteobjekt aus und klicken Sie auf das Symbol  .

Engine-Steuerungswerte

Die Engine-Steuerelementwerte sind eine Möglichkeit, bestimmte Standardverhalten der Identity Manager-Engine zu ändern. Auf die Werte kann nur zugegriffen werden, wenn ein Server mit dem Treibersatzobjekt verknüpft ist.

Option	Beschreibung
Subscriber channel retry interval in seconds (Wiederholintervall für Abonnentenkanal in Sekunden)	Das Wiederholintervall für den Abonnentenkanal steuert, wie häufig die Identity Manager-Engine die Verarbeitung einer zwischengespeicherten Transaktion wiederholt, nachdem das Abonnentenobjekt des Anwendungs-Shim einen Wiederholungsstatus zurückgegeben hat.
Qualified form for DN-syntax attribute values (Qualifizierte Form für DN-Syntax-Attributwerte)	Das Steuerelement für die qualifizierte Form der DN-Syntax-Attributwerte steuert, ob Werte für die DN-Syntax-Attributwerte in nicht qualifizierter Schrägstrichform oder in qualifizierter Schrägstrichform dargestellt werden. Wenn dies auf „true“ (wahr) festgelegt ist, werden die Werte in qualifizierter Form dargestellt.
Qualified form from rename events (Qualifizierte Form von Umbenennungsereignissen)	Das Steuerelement für die qualifizierte Form für Umbenennungsereignisse steuert, ob der neue Namensteil eines Umbenennungsereignisses aus dem Identitätsdepot dem Abonnentenkanal mit Typqualifizierern präsentiert wird. Beispiel: CN=. Wenn dies auf „true“ (wahr) festgelegt ist, werden die Namen in qualifizierter Form dargestellt.
Maximum eDirectory replication wait time in seconds (Maximale Wartezeit in Sekunden für die eDirectory-Replikation)	Dieses Steuerelement steuert die maximale Zeit, während der die Identity Manager-Engine auf die Replikation einer Änderung zwischen dem lokalen Replikat und dem Remote-Replikat wartet. Dies betrifft nur Vorgänge, bei denen die Identity Manager-Engine zum Ausführen des Vorgangs einen eDirectory-Remoteserver im selben Baum kontaktieren muss und zum Abschließen des Vorgangs möglicherweise warten muss, bis eine Änderung auf dem bzw. vom Remoteserver repliziert wurde (z. B. Verschieben eines Objekts, wenn der Identity Manager-Server nicht das Masterreplikat des verschobenen Objekts enthält oder Vorgänge für Dateisystemrechte für Benutzer, die aus einer Schablone erstellt wurden).
Use non-compliant backwards-compatible mode for XSLT (Nicht konformen abwärtskompatiblen Modus für XSLT verwenden)	Dieses Steuerelement setzt den von der Identity Manager-Engine verwendeten XSLT-Prozessor in einen abwärtskompatiblen Modus. Im abwärtskompatiblen Modus weist der XSLT-Prozessor ein Verhalten auf, das nicht mit XPath 1.0 und XSLT 1.0 konform ist. Dies erfolgt aus Gründen der Abwärtskompatibilität mit vorhandenen DirXML-Formatvorlagen, die von diesem nicht standardmäßigen Verhalten abhängen. Zum Beispiel ist das Verhalten des XPath-Operators „!=“ in DirXML-Versionen bis einschließlich Identity Manager 2.0 falsch, wenn einer der Operanden den Typ „node-set“ und der andere Operand einen anderen Typ aufweist. Dieses Verhalten wurde korrigiert, aber das korrigierte Verhalten wird mit dieser Option standardmäßig deaktiviert, um die Abwärtskompatibilität mit vorhandenen DirXML-Formatvorlagen zu gewährleisten.

Option	Beschreibung
Höchstzahl der Anwendungsobjekte, die gleichzeitig migriert werden	Mit diesem Steuerelement begrenzen Sie die Anzahl der Anwendungsobjekte, die die Identity Manager-Engine während einer einzelnen Abfrage, die als Teil des Migrierens von Objekten aus der Anwendung ausgeführt wird, von der Anwendung anfordern kann. Wenn java.lang.OutOfMemoryError-Fehler während einer Migration von einer Anwendung auftreten, sollte diese Zahl auf einen kleineren Wert als die Standardeinstellung festgelegt werden. Der Standardwert ist 50. **HINWEIS:** Dieses Steuerelement begrenzt nicht die Anzahl der Anwendungsobjekte, die migriert werden können, sondern lediglich die Stapelgröße.
Set creatorsName on objects created in Identity Vault (creatorsName-Attribut für im Identitätsdepot erstellte Objekte festlegen)	Mit diesem Steuerelement ermittelt die Identity Manager-Engine, ob das Attribut „creatorsName“ für alle von einem Treiber im Identitätsdepot erstellten Objekte auf den DN dieses Treibers festgelegt werden soll. Die Festlegung des Attributs „creatorsName“ ermöglicht ein einfaches Identifizieren der von diesem Treiber erstellten Objekte, bringt jedoch auch Leistungseinbußen mit sich. Wenn dieses Steuerelement nicht festgelegt wird, wird das Attribut „creatorsName“ standardmäßig auf den DN des NCP-Serverobjekts gesetzt, das als Host des Treibers dient.
Write pending associations (Ausstehende Verknüpfungen schreiben)	Dieses Steuerelement legt fest, ob die Identity Manager-Engine während der Verarbeitung des Abonnentenkanals eine ausstehende Verknüpfung für ein Objekt schreibt. Das Schreiben einer ausstehenden Verknüpfung bringt wenig oder gar keinen Nutzen und ist mit Leistungseinbußen verbunden. Zur Gewährleistung der Abwärtskompatibilität besteht jedoch die Möglichkeit, dies zu aktivieren.
Use password event values (Passwortereigniswerte verwenden)	Dieses Steuerelement legt den Ursprung des Werts fest, der für das Attribut „nspmDistributionPassword“ für Hinzufügungs- und Änderungsereignisse des Abonnentenkanals gemeldet wird. Wenn das Steuerelement auf „false“ (falsch) festgelegt wird, wird der aktuelle Wert von „nspmDistributionPassword“ genommen und als Wert des Attributereignisses gemeldet. Dies bedeutet, dass nur der aktuelle Passwortwert verfügbar ist. Dies ist das Standardverhalten. Wenn das Steuerelement auf „true“ (wahr) festgelegt wird, wird der mit dem eDirectory-Ereignis aufgezeichnete Wert entschlüsselt und als Wert des Attributereignisses gemeldet. Dies bedeutet, dass sowohl der alte Passwortwert (sofern vorhanden) und der neue Passwortwert zum Zeitpunkt des Ereignisses verfügbar sind. Dies ist zur Passwortsynchronisierung bei den Anwendungen hilfreich, die zum Festlegen eines neuen Passworts das alte Passwort benötigen.
Retry Out of Band events (Out-of-Band-Ereignisse wiederholen)	Dieses Steuerelement legt fest, ob die Out-of-Band-Synchronisierungsereignisse wiederholt werden sollen, wenn für das Out-of-Band-Synchronisierungsereignis der Status **Wiederholen** empfangen wird. Wenn das Steuerelement auf „false“ (falsch) festgelegt ist, wird die Out-of-Band-Synchronisierung nicht wiederholt. Wenn es auf „true“ (wahr) gesetzt ist, wird die Out-of-Band-Synchronisierung wiederholt, bis sie erfolgreich ist.

Option	Beschreibung
Use Rhino ECMAScript engine (Rhino-ECMA-Skript-Engine verwenden)	Legt fest, ob die Identity Manager-Engine die Rhino-ECMA-Skript-Engine verwendet. Die Engine verwendet Rhino als standardmäßige ECMA-Skript-Engine. Dieses Steuerelement ist standardmäßig auf **true** (wahr) festgelegt. Wenn Sie das Steuerelement auf **false** (falsch) setzen, verwendet die Engine das Nashorm-Skript.
Abonnentendienstkanal aktivieren	Legt fest, ob die Identity Manager-Engine die Out-of-Band-Abfragen auf dem Abonnentenservicekanal des Treibers verarbeitet. Beispiele für solche Abfragen sind Codezuordnungsaktualisierungen, Datensammlungen und Abfragen, die von dxcmd ausgelöst werden. Wenn dieses Steuerelement auf „true“ (wahr) festgelegt ist, verarbeitet der Kanal diese Abfragen separat, ohne die normale Verarbeitung von Ereignissen zu unterbrechen. Zurzeit ist dieses Steuerelement nur für die Verwendung mit dem JDBC-Auffächerungstreiber verfügbar (standardmäßig aktiviert).
Enable password synchronization status reporting (Berichte zum Passwortsynchronisierungsstatus aktivieren)	Dieses Steuerelement legt fest, ob die Identity Manager-Engine den Status von Passwortänderungsereignissen für den Abonnentenkanal meldet. Das Melden des Status der Passwortänderungsereignisse für den Abonnentenkanal ermöglicht es Anwendungen wie der Identity Manager-Benutzeranwendung, den Synchronisierungsfortschritt einer Passwortänderung für die verbundene Anwendung zu überwachen.
Combine values from template object with those from add operation (Werte aus Schablonenobjekt mit Werten aus Hinzufügungsvorgang kombinieren)	Dieser Wert legt fest, ob die Identity Manager-Engine beim Hinzufügen ähnliche Werte aus einer Erstellungsschablone und einen Hinzufügungsvorgang kombiniert. Ist der Wert auf "Wahr" gesetzt, werden die Attributwerte aus der Schablone, die jeweils aus mehreren Werten bestehen können, zusätzlich zu den im Hinzufügevorgang angegebenen Werten für dasselbe Attribut verwendet. Ist der Wert auf „false“ (falsch) gesetzt, werden die Werte aus der Schablone ignoriert, wenn Werte für dasselbe Attribut im Hinzufügungsvorgang angegeben sind.
Allow event loopback from publisher to subscriber channel (Ereignis-Loopback vom Herausgeber- zum Abonnentenkanal zulassen)	Dieser Wert legt fest, ob die Identity Manager-Engine zulässt, dass ein Ereignis vom Herausgeberkanal des Treibers zum Abonnentenkanal zurückführt. Wenn "Falsch", lässt die Identity Manager-Engine kein Ereignis-Loopback zu. Wenn der Wert auf „true“ (wahr) gesetzt ist, lässt die Identity Manager-Engine zu, dass Ereignisse vom Herausgeberkanal zum Abonnentenkanal zurückführen.

Option	Beschreibung
Revert to calculated membership value behavior (Auf Verhalten des berechneten Mitgliedschaftswerts zurücksetzen)	Dieser Wert legt fest, welche Methode die Identity Manager-Engine beim Lesen und Suchen von Werten, die sich auf die Gruppenmitgliedschaft beziehen, anwendet. Wenn der Wert auf „false“ (falsch) gesetzt ist (Standardeinstellung), gibt die Identity Manager-Engine beim Lesen bzw. Suchen der Attribute „Mitglied“ und „Gruppenmitgliedschaft“ von Identitätsdepotobjekten ausschließlich die „statischen“ Werte zurück. Statische Werte sind Objekte, die die Gruppenmitgliedschaft durch die Direktzuweisung zur Gruppe, anstatt über eine geerbte Zuweisung durch eine verschachtelte Gruppe erworben haben. Wenn der Wert auf „true“ (wahr) gesetzt ist, kehrt die Identity Manager-Engine zum Verfahren zurück, die in Versionen vor Identity Manager 3.6 angewendet wurde. In Versionen unter 3.6 ruft die Identity Manager-Engine bei einer Suche nach den Attributen „Mitglied“ und „Gruppenmitgliedschaft“ alle „berechneten“ Werte ab. Berechnete Werte umfassen Objekte, die aufgrund der Hierarchie-Berechnungen der verschachtelten Gruppen von eDirectory entweder über eine 1) statisch beauftragte Mitgliedschaft oder 2) dynamisch beauftragte Mitgliedschaft verfügen. Bei der Suche nach dem Gruppenmitgliedsattribut werden in diesem Fall alle Objekte zurückgegeben, die der Gruppe direkt zugewiesen sind oder denen die Mitgliedschaft über eine verschachtelte Gruppe zugewiesen wurde.
Maximum time to wait for driver shutdown in seconds (Maximale Wartezeit für Herunterfahren des Treibers in Sekunden)	Diese Einstellung steuert, wie lange die Identity Manager-Engine maximal auf das Herunterfahren des Treibers durch den Herausgeberkanal wartet. Wenn der Treiber nicht innerhalb des angegebenen Zeitintervalls heruntergefahren wird, beendet die Identity Manager-Engine den Treiber.
Regular Expression escape meta-characters (Escapezeichen für Metazeichen in regulären Ausdrücken)	Dieses Steuerelement bestimmt die Metazeichen, die beim Erweitern der lokalen Variable bei Verwendung in einem Kontext regulärer Ausdrücke mit Escapezeichen versehen werden. Alle Zeichen, die mit Escapezeichen versehen werden müssen, müssen als durch Kommas getrennte Liste für diesen Steuerelementwert hinzugefügt werden. Wenn ein Metazeichen nicht im Steuerelementwert vorhanden ist, wird es während der Erweiterung lokaler Variablen, die einen regulären Ausdruck enthalten, nicht mit Escapezeichen versehen. Stellen Sie bei der Verwendung dieses Steuerelements Folgendes sicher: ◆ Der Wert wird nicht leer gelassen. Standardmäßig ist der Wert mit ***$*** ausgefüllt. Dieses Zeichen ist für die Erweiterung lokaler Variablen erforderlich. ◆ Der Wert muss eine gültige Liste durch Kommas (,) getrennter Werte sein. Andernfalls treten bei der Richtlinienauswertung Fehler auf. ◆ Um alle Metazeichen mit Escapezeichen zu versehen, geben Sie Folgendes als Wert an: "\,$,^,.,?,*,+,[,],(,),|". ◆ Wenn ein Metazeichen nicht mit Escapezeichen versehen werden muss, entfernen Sie dieses Zeichen aus dem Wert. ◆ Um ein beliebiges Metazeichen mit Escapezeichen zu versehen, geben Sie das Metazeichen gefolgt von einem umgekehrten Schrägstrich (\) an.

Option	Beschreibung
Ignore Entitlement Changes of other drivers (Berechtigungsänderungen anderer Treiber ignorieren)	Dieses Steuerelement legt fest, ob die Identity Manager-Engine Berechtigungsänderungen anderer Treiber ignoriert oder verarbeitet. Der Standardwert ist "Wahr". Das bedeutet, dass der Treiber die Berechtigungsänderungen anderer Treiber automatisch ignoriert. Wenn dieses Steuerelement auf „false“ (falsch) festgelegt ist, werden die Berechtigungsänderungen anderer Treiber im Cache gespeichert und von diesem Treiber verarbeitet.
Allow Entitlement event loopback from cprs to subscriber channel (Berechtigungsereignis-Loopback von cprs zum Abonnentenkanal zulassen)	Dieses Steuerelement legt fest, ob die Identity Manager-Engine zulässt, dass ein Berechtigungsereignis, das von einer CPRS-Zuweisung generiert wird, im Loopback zum Abonnentenkanal des Treibers zurückführt. Der Standardwert ist "Falsch". Das bedeutet, dass das Ereignis nicht zurück zum Abonnentenkanal zurückführt. Wenn dieses Steuerelement auf „true“ (wahr) gesetzt wird, fließt das Ereignis zum Abonnentenkanal des Treibers.

Startoptionen

Mit den Startoptionen können Sie den Treiberstatus beim Starten des Identity Manager-Servers festlegen.

- **Automatisch starten**: Der Treiber wird bei jedem Starten des Identity Manager-Servers gestartet.
- **Manuell**: Der Treiber wird beim Starten des Identity Manager-Servers nicht gestartet. Der Treiber muss über das Identity Console-Portal gestartet werden.
- **Deaktiviert**: Der Treiber verfügt über eine Cache-Datei, in der alle Ereignisse gespeichert werden. Wenn der Treiber auf „Deaktiviert“ festgelegt ist, wird diese Datei gelöscht und es werden keine neuen Ereignisse in der Datei gespeichert, bis der Treiberstatus auf „Manuell“ oder „Automatisch starten“ geändert wird.

Nachdem Sie die bevorzugte Startoption festgelegt haben, klicken Sie zum Speichern auf das Symbol  . Um die Startoption zurückzusetzen, klicken Sie auf das Symbol  .

Benanntes Passwort

Mit Identity Manager können Sie mehrere Passwörter für einen Treiber sicher speichern. Diese Funktionalität wird als „Benannte Passwörter“ bezeichnet. Der Zugriff auf die einzelnen Passwörter erfolgt über einen Schlüssel bzw. Namen.

Sie können benannte Passwörter zu einem Treibersatz oder zu einzelnen Treibern hinzufügen. Benannte Passwörter für einen Treibersatz sind für alle Treiber im Satz verfügbar. Benannte Passwörter für einen einzelnen Treiber sind nur für diesen spezifischen Treiber verfügbar.

Wenn Sie ein benanntes Passwort in einer Treiberrichtlinie verwenden möchten, verweisen Sie mit dem Namen des Passworts darauf, anstatt das eigentliche Passwort zu verwenden. Das Passwort wird dann über die Identity Manager-Engine an den Treiber gesendet. Die in diesem Abschnitt beschriebene Methode zum Speichern und Abrufen von benannten Passwörtern kann für alle Treiber verwendet werden, ohne dass Änderungen am Treiber-Shim erforderlich sind.

Um ein neues benanntes Passwort hinzuzufügen, klicken Sie auf das Symbol +. Um ein vorhandenes benanntes Passwort zu entfernen, klicken Sie auf das Symbol 🗑. Um die Liste zu speichern, klicken Sie auf das Symbol .

Sicherheitsäquivalenzen

Auf der Seite „Sicherheitsäquivalenzen“ können Sie die Liste der Objekte anzeigen oder ändern, für die der Treiber als Sicherheitsäquivalenz definiert ist. Dieses Objekt besitzt effektiv alle Rechte der aufgeführten Objekte.

Sie können ein neues Objekt zur Liste „Sicherheitsäquivalenzen“ hinzufügen, indem Sie auf das Symbol + klicken. Wenn Sie ein Objekt zur Liste hinzufügen oder aus ihr löschen, fügt das System dieses Objekt automatisch zur Eigenschaft „Sicherheit entspricht mir“ des Objekts hinzu bzw. löscht es daraus. Es ist nicht erforderlich, den Trustee [Öffentlich] oder die übergeordneten Container dieses Objekts zur Liste hinzuzufügen, weil dieses Objekt bereits implizit sicherheitsäquivalent zu diesen Elementen ist.

Um ein vorhandenes Objekt aus dieser Liste zu entfernen, klicken Sie auf das Symbol 🗑. Um die Liste zu speichern, klicken Sie auf das Symbol .

Ausgeschlossene Objekte

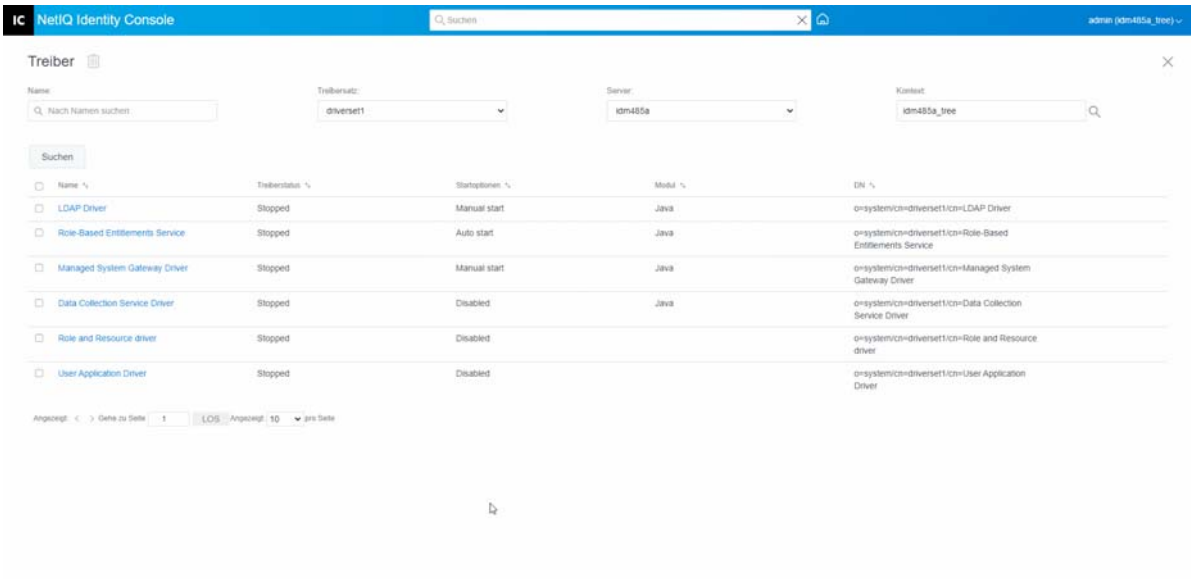
Mit dieser Option können Sie eine Liste der Objekte erstellen, die nicht zur Anwendung repliziert werden sollen. Es wird empfohlen, dass Sie dieser Liste alle Objekte hinzufügen, die administrativ relevant sind (z. B. das ADMIN-Objekt). Sie können ein neues Objekt zu dieser Liste hinzufügen, indem Sie auf das Symbol + klicken. Um ein vorhandenes Objekt aus dieser Liste zu entfernen, klicken Sie auf das Symbol 🗑. Um die Liste zu speichern, klicken Sie auf das Symbol .

Liste der Attribute mit Wert verwalten

Führen Sie die folgenden Schritte aus, um für einen bestimmten Treiber Attribute zur Liste der Attribute mit Wert hinzuzufügen:

1. Wählen Sie in Identity Console das Modul **Objektverwaltung** aus.
2. Wählen Sie den Typ **DirXML-Driver** (DirXML-Treiber) aus der Dropdown-Liste aus und klicken Sie auf die Suchschaltfläche.
3. Klicken Sie in der Suchliste auf den entsprechenden Treiber.
4. Um Attribute ohne Wert zur Liste der Attribute mit Wert hinzuzufügen, klicken Sie auf das Symbol + neben **Attribute mit Wert** und wählen Sie die entsprechenden Attribute ohne Wert aus der Liste aus.
5. Wenn Sie fertig sind, klicken Sie auf **OK**.

Abbildung 23-2 *Treiberkonfiguration verwalten*



Datentransformation und -synchronisierung

Dieser Abschnitt behandelt die folgenden Themen:

- „Datensynchronisierungsansicht“, auf Seite 164
- „Klassen-/Attributfilter“, auf Seite 167
- „ECMA-Skript“, auf Seite 168
- „Zuordnung wechselseitiger Attribute“, auf Seite 168

Datensynchronisierungsansicht

Die Übersichtsseite des Treibers ist in die folgenden Kategorien unterteilt:

- „Filter“, auf Seite 165
- „Alle Richtlinien“, auf Seite 165
- „Daten in das Identitätsdepot migrieren“, auf Seite 165
- „Daten aus dem Identitätsdepot migrieren“, auf Seite 166
- „Objekte synchronisieren“, auf Seite 166
- „DirXML-Skript-Tracing“, auf Seite 166

Filter

Der Treiber enthält Filter, mit denen Sie festlegen können, welche Klassen und Attribute einer Anwendung Daten an ein Identitätsdepot senden bzw. von diesem empfangen können. Wenn eine bestimmte Klasse zur Verarbeitung an die Metaverzeichnis-Engine übergeben werden soll, sollten Sie die Klasse im entsprechenden Kanal zum Filter hinzufügen. Sie können Objekte auch nach einem bestimmten Attributwert filtern, den Sie definieren.

Um Klassen und Attribute hinzuzufügen, die für die Synchronisierung einbezogen werden sollen, und den Treiberfilter zu ändern, klicken Sie im Herausgeber- oder Abonnentenkanal auf **Filter**.

HINWEIS: Die grafische Darstellung des Überblicks zeigt für den Treiberfilter im Herausgeber- und Abonnentenkanal zwei separate Objekte. Obwohl zwei Objekte angezeigt werden, wird für beide Kanäle derselbe Filter verwendet.

Alle Richtlinien

Standardmäßig wird die Seite „Alle Richtlinien“ angezeigt. Sie können eine vorhandene Richtlinie in den Container importieren, indem Sie auf das Symbol klicken. Sie können auch jede beliebige Richtlinie entfernen, die nicht erforderlich ist. Um eine Trace-Stufe für den Treiber auszuwählen, klicken Sie auf das Symbol . Sie können die Richtlinien in der Liste nach oben und unten verschieben, indem Sie die Symbole und verwenden.

HINWEIS: Das Hinzufügen und Bereitstellen neuer Richtlinien für Treiber wird mit Identity Console nicht unterstützt. Es wird empfohlen, iManager und Identity Designer zum Hinzufügen und Bereitstellen neuer Richtlinien zu verwenden.

Daten in das Identitätsdepot migrieren

Mit dieser Aufgabe definieren Sie die Kriterien, die Identity Manager verwendet, um Objekte aus einer Anwendung in das Identitätsdepot zu migrieren. Wenn Sie ein Objekt migrieren, wendet die Metaverzeichnis-Engine alle Entsprechung-, Platzierungs- und Erstellungsrichtlinien sowie den Herausgeberfilter auf das Objekt an. Objekte werden in der Reihenfolge in das Identitätsdepot migriert, in der sie in der Liste der Klassen angegeben sind. Mit dieser Option können Sie die folgenden Aufgaben ausführen:

1. **Klassen und Attribute hinzufügen**: Klicken Sie auf das Symbol , um zu migrierende Klassen oder Attribute hinzuzufügen oder zu entfernen. Wählen Sie dann die Klasse und die entsprechenden Attribute aus, die Sie hinzufügen möchten. Nachdem Sie die Klasse und die Attribute ausgewählt haben, klicken Sie auf **Hinzufügen**, um die Änderungen zu speichern.
2. **Attributwert bearbeiten**: Um den Migrationsattributwert zu ändern, den Sie beim Bearbeiten der Liste angegeben haben, klicken Sie auf das Attributbearbeitungssymbol .
3. **Klassenliste neu ordnen**: Mit den Schaltflächen und können Sie die Reihenfolge der Klassen in der Liste ändern. Objekte werden in der Reihenfolge in das Identitätsdepot migriert, in der sie in der Liste der Klassen angegeben sind.
4. **Aktualisieren:** Klicken Sie auf das Symbol , um die Liste zu aktualisieren.

Daten aus dem Identitätsdepot migrieren

Auf der Registerkarte **Exportieren** können Sie Container oder Objekte auswählen, die Sie vom Identitätsdepot zu einer Anwendung migrieren möchten. Wenn Sie ein Objekt migrieren, wendet die Metaverzeichnis-Engine alle Entsprechung-, Erstellungs- und Platzierungsrichtlinien sowie den Abonnentenfilter auf das Objekt an.

Um Objekte oder Container aus dem Identitätsdepot in eine andere Anwendung zu migrieren, klicken Sie auf das Symbol  . Wählen Sie das zu migrierende Objekt durch Durchsuchen aus und klicken Sie anschließend auf **OK**, um das Objekt zur Migrationsliste hinzuzufügen. Um Objekte aus der Migrationsliste zu entfernen, klicken Sie auf das Symbol  .

Wenn Sie die zu migrierenden Objekte ausgewählt haben, klicken Sie auf  , um den Migrationsvorgang zu starten. Der Migrationsfortschritt wird auf dem Bildschirm angezeigt. Wenn Sie die Migration beenden möchten, klicken Sie auf die Schaltfläche  .

Objekte synchronisieren

Der Synchronisierungsvorgang sucht nach Objekten, die geändert wurden, und synchronisiert sie. Sie können **Alle Objekte untersuchen** auswählen, um die Synchronisierung sofort zu starten. Alternativ können Sie ein Datum/eine Uhrzeit für den Beginn der Synchronisierung festlegen.

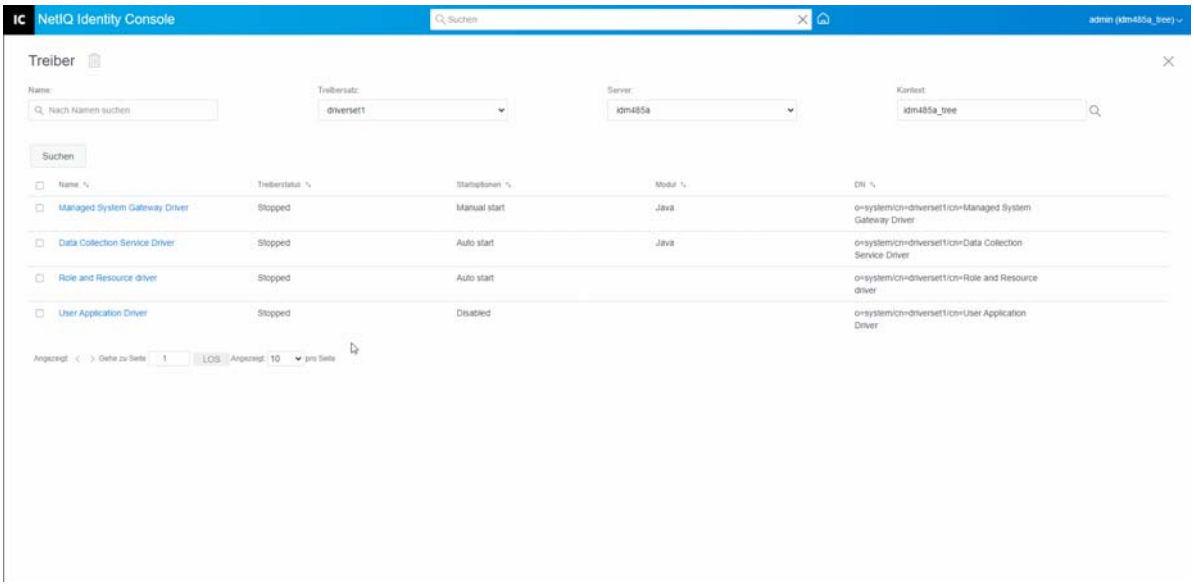
DirXML-Skript-Tracing

Mit der Option des DirXML-Skript-Tracing können Sie eine Trace-Stufe für einen Treiber auswählen. Die Trace-Einstellungen werden auch auf alle Herausgeber- und Abonnentenkanäle angewendet. Für das DirXML-Skript-Tracing stehen die folgenden Optionen zur Auswahl:

- Gesamtes DirXML-Skript-Tracing aktiviert
- Gesamtes DirXML-Skript-Tracing deaktiviert
- DirXML-Skriptregel-Tracing aktiviert
- DirXML-Skriptregel-Tracing deaktiviert

Klicken Sie zum Speichern der Änderungen auf  .

Abbildung 23-3 *Datensynchronisierung von Treibern verwalten*



Klassen-/Attributfilter

Mit den Klassen-/Attributfiltern können Sie angeben, welche Klassen und Attribute eine Anwendung an das Identitätsdepot senden bzw. von diesem empfangen kann. Wenn eine bestimmte Klasse zur Verarbeitung an die Metaverzeichnis-Engine übergeben werden soll, sollten Sie die Klasse im entsprechenden Kanal zum Filter hinzufügen. Außerdem können Sie Objekte nach einem von Ihnen definierten Attributwert filtern. Mit dieser Option können Sie die folgenden Aktionen ausführen:

- **Schablone festlegen**: Mit dieser Option legen Sie die Standardoptionen für alle Attribute fest, die zum Filter hinzugefügt werden. Klicken Sie auf das Symbol neben der Bezeichnung „Klassen-/Attributfilter“.
- **Neue Klasse hinzufügen**: Fügen Sie eine neue Klasse hinzu, indem Sie auf das Symbol klicken.
- **Neues Attribut hinzufügen**: Fügen Sie ein neues Attribut hinzu, indem Sie auf das Symbol klicken.
- **Filter kopieren von**: Mit dieser Option können Sie einen Filter von einem anderen Treiber kopieren. Klicken Sie auf das Symbol , um den Filter zu kopieren.
- **XML bearbeiten**: Sie können die Einstellungen für Klassen- und Attributfilter über das Symbol für die Bearbeitung von XML-Dateien bearbeiten.
- **Klassen oder Attribute löschen**: Um eine Klasse oder ein Attribut zu löschen, klicken Sie auf das Symbol neben der entsprechenden Klasse bzw. dem entsprechenden Attribut.

Sie können die folgenden Optionen für einen Klassen- oder Attributwert im Herausgeberkanal und im Abonnentenkanal festlegen:

- Synchronisieren
- Ignorieren

- Notify
- Zurücksetzen

Zusammenführungsstelle

Wenn ein Attribut in keinem der beiden Kanäle synchronisiert wird, findet keine Zusammenführung statt.

Wenn ein Attribut in einem, aber nicht im anderen Kanal synchronisiert wird, werden alle vorhandenen Werte auf der Zielseite dieses Kanals entfernt und durch die Werte aus dem Ursprung dieses Kanals ersetzt. Wenn der Ursprung über mehrere Werte verfügt und das Ziel nur einen Wert aufnehmen kann, wird auf der Zielseite nur einer dieser Werte verwendet.

Wenn ein Attribut in beiden Kanälen synchronisiert wird und beide Seiten nur einen Wert aufnehmen können, übernimmt die verbundene Anwendung die Werte aus dem Identitätsdepot, es sein denn, dort sind keine gespeicherten Werte vorhanden. In diesem Szenario ruft das Identitätsdepot die Werte von der verbundenen Anwendung ab.

Wenn ein Attribut in beiden Kanälen synchronisiert wird und nur eine Seite mehrere Werte aufnehmen kann, wird der Wert aus dem einwertigen Kanal zum mehrwertigen Kanal hinzugefügt, sofern der Wert dort noch nicht vorhanden ist. Wenn auf der Seite, die nur einen Wert aufnehmen kann, kein Wert vorhanden ist, können Sie einen Wert auswählen, der dieser Seite hinzugefügt werden soll. Sie können die folgenden Optionen für „Zertifizierungsstelle zusammenführen“ festlegen:

- Standard
- Identitätsdepot
- Anwendung
- Keine

Klicken Sie zum Speichern der Änderungen auf  .

ECMA-Skript

Zeigt eine geordnete Liste der ECMA-Skript-Ressourcendateien an. Die Dateien enthalten die Erweiterungsfunktionen für den Treiber, die Identity Manager beim Starten des Treibers lädt. Sie können zusätzliche Dateien importieren, indem Sie auf  klicken, vorhandene Dateien entfernen, indem Sie auf  klicken, oder die Reihenfolge der ausgeführten Dateien ändern. Sie können die Skripte auch in der Liste nach oben und unten verschieben. Sie können die ECMA-Skriptliste speichern, indem Sie auf das Symbol  klicken.

Zuordnung wechselseitiger Attribute

Bei der Zuordnung wechselseitiger Attribute können sie die Backlinks bzw. Verweise zwischen den Objekten erstellen und verwalten. Das Objekt "Gruppe" verfügt beispielsweise über das Attribut "Mitglieder", das sich auf alle Benutzerobjekte bezieht, die dieser Gruppe angehören. Weiterhin hat jedes Benutzerobjekt das Attribut "Gruppenmitgliedschaft", das auf die Gruppen verweist, bei denen der betreffende Benutzer Mitglied ist. Damit eine Synchronisierung zwischen "Gruppenobjekt

> Attribut 'Mitglieder'" und "Benutzerobjekt > Attribut 'Gruppenmitgliedschaft'" für alle Gruppen- und Benutzerobjekte im Identitätsdepot durch die Metaverzeichnis-Engine möglich ist, müssen diese Attribute verknüpft werden. Diese Verknüpfungen zwischen Objektattributen werden als "Zuordnungen von wechselseitigen Attributen" bezeichnet.

Mit diesem Modul können Sie die folgenden Aktionen ausführen:

Benutzerdefinierte Zuordnung reziproker Attribute erstellen

Dieser Abschnitt gilt nur, wenn auf der Seite „Zuordnungen reziproker Attribute“ die Aufforderung **Der Treiber enthält keine benutzerdefinierten Zuordnungen reziproker Attribute. Klicken Sie oben auf das Symbol '+', um Grundzuordnungen reziproker Attribute zu erstellen** angezeigt wird.

1. Klicken Sie auf das Symbol +, um eine neue benutzerdefinierte Zuordnungsliste für reziproke Attribute zu erstellen.
2. Die Standardattributzuordnungen des Treibers werden angezeigt. Sie können nun Zuordnungen hinzufügen, die vorhandenen Zuordnungen ändern oder Zuordnungen löschen.

Neue Zuordnung reziproker Attribute hinzufügen

Wenn Sie eine Zuordnung reziproker Attribute erstellen, müssen Sie zuerst eines der Attribute zur Liste der Zuordnungen reziproker Attribute hinzufügen.

1. Klicken Sie auf das Symbol + neben dem Dropdown-Menü „Aktionen“.
2. Wählen Sie im neuen Attributeintrag das gewünschte Attribut aus der Dropdown-Liste aus.
3. Geben Sie die Details der reziproken Zuordnung an:
   - 3a **Ursprungsklasse**: Gibt den Namen der Klasse an, mit der das Attribut in der Zuordnungsliste verknüpft ist. Wenn Sie z. B. das Attribut „Gruppenmitgliedschaft“ in die Liste der reziproken Zuordnung platziert haben, lautet die verknüpfte Ursprungsklasse „Benutzer“.
   - 3b **Zielklasse**: Gibt den Namen der Klasse an, die mit dem Attribut verknüpft ist, zu dem Sie eine reziproke Zuordnung erstellen möchten. Wenn Sie z. B. das Attribut „Gruppenmitgliedschaft“ in die Liste der reziproken Zuordnung platziert haben, lautet die verknüpfte Zielklasse „Gruppe“.
   - 3c **Reziprokes Attribut**: Gibt den Namen des Attributs an, zu dem eine reziproke Zuordnung erstellt werden soll.

4 Wenn Sie das Attribut einem anderen wechselseitigen Attribut zuordnen möchten, klicken Sie auf das Symbol + rechts neben dem Attributnamen.

Am Ende der Attributliste wird ein neuer Abschnitt für das Attribut eingefügt. Wählen Sie die Ursprungsklasse, die Zielklasse und das wechselseitige Attribut aus.

Zuordnung reziproker Attribute entfernen

So entfernen Sie eine Zuordnung reziproker Attribute:

1 Aktivieren Sie das Kontrollkästchen vor **Ursprungsklasse** für die Zuordnung reziproker Attribute, die Sie löschen möchten.

2 Klicken Sie auf das Symbol 🗑 neben der Dropdown-Liste „Attribute“.

Attribute aus der Liste einer Zuordnung reziproker Attribute entfernen

So entfernen Sie ein Attribut aus der Liste der reziproken Zuordnung:

1 Wählen Sie das Attribut aus, das Sie entfernen möchten, indem Sie das Kontrollkästchen vor dem Attribut aktivieren.

2 Klicken Sie auf das Symbol 🗑 neben der Dropdown-Liste **Attribute**.

Zugeordnete Attribute neu ordnen

Die Attributzuordnungen werden in der aufgeführten Reihenfolge von oben nach unten aufgelöst. Sie können die zugeordneten Attribute in der Liste nach oben oder unten verschieben, um sicherzustellen, dass sie in der richtigen Reihenfolge aufgelöst werden. Im Allgemeinen sollten zuerst spezifische Zuordnungen und anschließend allgemeinere Zuordnungen aufgeführt sein. Eine Zuordnung für das Mitgliedsattribut eines Gruppenobjekts sollte beispielsweise vor einer Zuordnung für das Mitgliedsattribut von beliebigen Objekten (der Option <Beliebige Klasse>) aufgeführt sein.

Wählen Sie das Kontrollkästchen vor dem zugeordneten Attribut aus, das Sie entfernen möchten, und klicken Sie anschließend auf ↑, um das Attribut nach oben, bzw. auf ↓, um es nach unten zu verschieben.

Benutzerdefinierte Zuordnungen reziproker Attribute entfernen

Sie können die benutzerdefinierten Attributzuordnungen, die Sie erstellt haben, auch wieder löschen. Dies führt dazu, dass die Metaverzeichnis-Engine die Standardattributzuordnungen für den Treiber verwendet.

Um eine benutzerdefinierte Zuordnung reziproker Attribute zu entfernen, klicken Sie oben im Bildschirm auf das Symbol 🗑.

XML der Zuordnungen reziproker Attribute bearbeiten

Falls gewünscht, können Sie den XML-Code für ein reziprokes Attribut direkt bearbeiten. Klicken Sie dazu auf der Seite „Benutzerdefinierte Zuordnungen reziproker Attribute“ auf das Symbol „XML bearbeiten“  . Dadurch wird ein einfacher XML-Editor geöffnet, mit dem Sie den XML-Code ändern können. Wenn Sie fertig sind, klicken Sie auf „OK“ oder „Abbrechen“, um den XML-Editor zu schließen.

Erweiterte Einstellungen

Die erweiterten Einstellungen sind in die folgenden Kategorien unterteilt:

- „Berechtigungen verwalten“, auf Seite 171
- „Objektzuordnungstabelle verwalten“, auf Seite 171
- „Aufträge für Treiber verwalten“, auf Seite 172

Berechtigungen verwalten

Die Seite „Berechtigungen“ enthält eine Tabelle mit allen Berechtigungen, die aktuell im ausgewählten Treiber (mit dem eindeutigen Namen aufgelistet) definiert sind. Auf dieser Seite sind die folgenden Aktionen möglich:

- **Im XML bearbeiten**: Um die Berechtigungen in der XML-Datei zu bearbeiten, wählen Sie die Berechtigung aus der Liste aus und klicken Sie auf das Symbol  . Aktivieren Sie dann das Kontrollkästchen **Enable XML Editing** (XML-Bearbeitung aktivieren).
- **Löschen**: Um eine Berechtigung zu löschen, aktivieren Sie das Kontrollkästchen links neben dem Berechtigungsnamen und klicken Sie auf das Symbol  . Es wird eine Meldung angezeigt, dass die Operation nicht rückgängig gemacht werden kann, und Sie werden gefragt, ob Sie sicher sind, dass Sie die ausgewählte Berechtigung löschen möchten. Klicken Sie auf **OK**, um die Berechtigung zu löschen, oder auf **Abbrechen**, um den Vorgang abzubrechen. Sie können auch mehrere Kontrollkästchen aktivieren, um mehrere Berechtigungen zu löschen, oder das Kontrollkästchen oben links aktivieren, um alle Berechtigungen zu löschen.

Objektzuordnungstabelle verwalten

Identity Manager-Richtlinien verwenden Zuordnungstabellen, um einen Wertesatz einem anderen entsprechenden Wertesatz zuzuordnen. Beim Installieren des Berechtigungspakets werden die Richtlinien dieses Pakets ui, Treiberstartrichtliniensatz hinzugefügt. Der Treiber führt diese Richtlinien nur einmal beim Starten des Treibers aus. Weitere Informationen finden Sie unter Mapping Table Objects (Tabellenobjekte zuordnen) im *NetIQ Identity Manager Driver Administration Guide* (NetIQ Identity Manager-Treiberadministrationshandbuch).

Mithilfe der Objektzuordnungstabelle können Sie die folgenden Aktionen ausführen:

- **Vorhandene Zuordnung löschen:** Um eine vorhandene Objektzuordnungstabelle zu ändern, klicken Sie in der Liste auf die Zuordnung und führen Sie auf dem nächsten Bildschirm die folgenden Aktionen aus:
  - Fügen Sie eine neue Spalte hinzu.

Geben Sie einen Wert für die Spalte an und wählen Sie, ob bei dem Wert die Groß- und Kleinschreibung beachtet wird oder ob er numerisch ist.

- Fügen Sie eine neue Zeile hinzu und geben Sie einen Wert für die Zeile an.
- Klicken Sie auf das Symbol .

- **Zuordnung löschen**: Um eine Zuordnung aus der Liste zu entfernen, wählen Sie die entsprechende Zuordnung aus der Liste aus und klicken Sie auf das Symbol .
- **In XML bearbeiten**: Um eine Zuordnung in der XML-Datei zu bearbeiten, klicken Sie in der Liste auf die Zuordnung und wählen Sie das Symbol aus. Aktivieren Sie dann das Kontrollkästchen **Enable XML Editing** (XML-Bearbeitung aktivieren).

Aufträge für Treiber verwalten

Mit der Option „Aufträge“ in Identity Console können Sie Ereignisse für alle einzelnen Treiber planen.

Die Seite „Job Scheduler“ (Auftragsplaner) enthält den Auftragsnamen, die Angabe, ob ein Auftrag aktiviert oder deaktiviert ist, zu welchem Zeitpunkt er ausgeführt werden soll sowie die Auftragsbeschreibung. Klicken Sie auf den Auftragsname, um die Seite "Auftrag" aufzurufen. Klicken Sie in der Spalte „Aktiviert“ auf das Symbol zum Aktivieren/Deaktivieren, um den Auftrag zu aktivieren bzw. zu deaktivieren. Klicken Sie auf die Auftragsbeschreibung, um die vollständige Beschreibung des Auftrags anzuzeigen.

Die Registerkarte „Aufträge“ enthält eine Tabelle mit den vorhandenen Auftragsobjekten für den ausgewählten Treiber, der mit dem vollständigen eindeutigen Namen (DN) im Treibereintrag aufgelistet wird.

Auf der Seite „Job Scheduler“ (Auftragsplaner) können Sie die folgenden Aufgaben ausführen:

- **Auftrag erstellen**: Klicken Sie auf das Symbol , um einen neuen Auftrag zu erstellen.

  Führen Sie im Popup-Fenster **Neuer Auftrag** die folgenden Schritte aus, um einen neuen Auftrag zu erstellen:

  1. Geben Sie den Auftragsnamen an.
  2. Wählen Sie den Auftragstyp aus.
  3. Klicken Sie auf das Symbol und wählen Sie in der Liste der verfügbaren Server den Server aus, auf dem Sie den Auftrag ausführen möchten. Geben Sie andernfalls einen Servernamen an und wählen Sie dann den Server aus.
  4. Klicken Sie auf die Schaltfläche **Erstellen**.
- **Auftrag starten**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .
- **Auftrag stoppen**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .
- **Auftrag aktivieren**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol .

- **Auftrag deaktivieren**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol ⊗.
- **Zustand abrufen**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol ⓘ.
- **Auftrag löschen**: Wählen Sie einen Auftrag aus, indem Sie auf das Feld links neben dem entsprechenden Auftrag klicken, und klicken Sie anschließend auf das Symbol 🗑.

Klicken Sie auf einen Auftrag, um die Seite **Auftragseigenschaften** aufzurufen. Hier können Sie festlegen, wie der Auftrag ausgeführt werden soll.

Allgemein: Zeigt den Java-Klassennamen für den Auftrag an. Auf dieser Seite können Sie einen Auftrag aktivieren oder deaktivieren, den Auftrag nach seiner Ausführung löschen, die Server auswählen, auf denen der Auftrag ausgeführt werden soll, den Email-Server angeben, einen anderen Anzeigenamen und eine andere Beschreibung für den Auftrag eingeben.

Zeitplan: Hier können Sie festlegen, wann der Auftrag ausgeführt werden soll. Geben Sie unter „Auftrag starten um“ die gewünschte Startuhrzeit an und legen Sie fest, ob der Auftrag täglich, wöchentlich, monatlich oder jährlich ausgeführt werden soll. Sie können auch benutzerdefiniert anpassen, wann Sie den Auftrag ausführen möchten, oder Sie können den Umschalter aktivieren, um den Auftrag manuell auszuführen.

Bereich: Mit dieser Option können Sie die Objekte definieren, für die dieser Auftrag gilt. Ein Objekt kann ein Container, eine dynamische Gruppe, eine Gruppe oder ein Blattobjekt sein. Klicken Sie auf "Hinzufügen", um ein Objekt auszuwählen, für das dieser Auftrag gilt. Wählen Sie ein Objekt aus, indem Sie auf die Schaltfläche "Durchsuchen" und anschließend auf "OK" klicken. Wählen Sie zum Entfernen einen Objekts aus der Liste "Bereich" das entsprechende Bereichsobjekt aus, indem Sie das Feld links neben dem DN-Objekt aktivieren und anschließend auf "Entfernen" klicken.

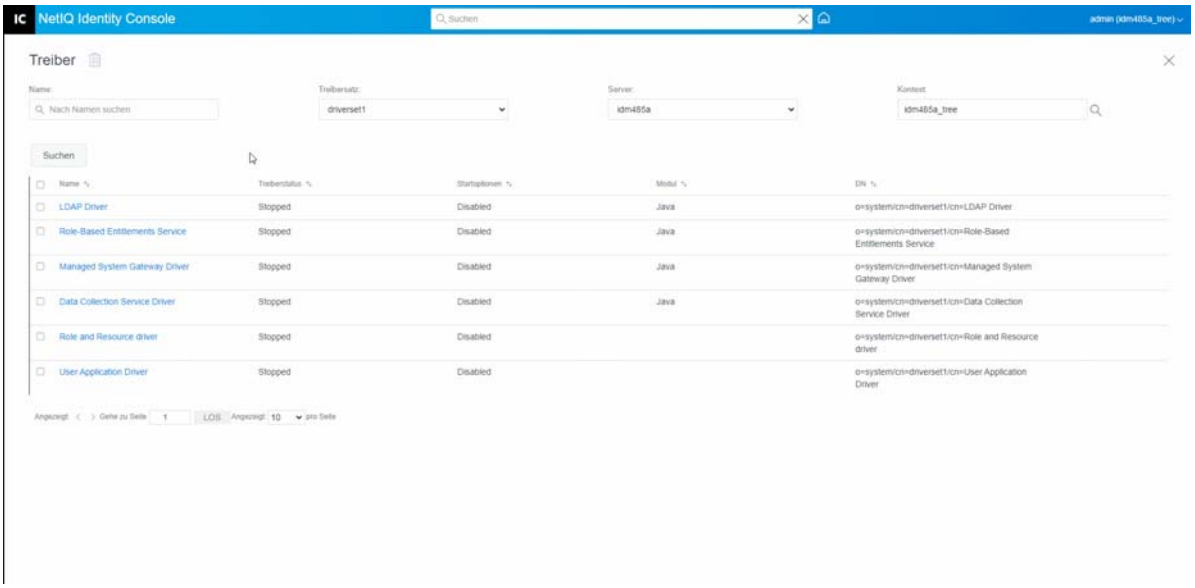
Wählen Sie ein hinzugefügtes Objekt aus, um weitere Optionen anzuzeigen. Bei Auswahl eines Gruppenobjekts können Sie den Auftrag entweder auf die Gruppenmitglieder oder nur auf die Gruppe anwenden. Bei Auswahl eines Containerobjekts können Sie den Auftrag auf alle nachgeordneten Einheiten im Container, auf alle untergeordneten Elemente im Container oder nur auf den Container anwenden.

Parameter: Mit dieser Option können Sie dem Auftrag zusätzliche Parameter hinzufügen und die zurzeit eingerichteten Parameter anzeigen. Je nach ausgewähltem Auftrag können sich diese Parameter ändern.

Ergebnisse: Mit dieser Option können Sie definieren, wie die Ergebnisse des Auftrags verarbeitet werden sollen. Die Seite "Ergebnisse" besteht aus zwei Teilen: "Zwischenergebnis" und "Endergebnis". Folgende Ergebnisse sind zulässig: "Erfolg", "Warnhinweis", "Fehler" und "Abgebrochen". Rechts neben der Spalte "Ergebnisse" befindet sich die Spalte "Aktion". Wenn Sie auf die Spalte "Aktion" klicken, können Sie den Benachrichtigungstyp für die einzelnen Ergebnisse festlegen. Zu den Aktionen gehören z. B. das Versenden eines Audit-Ergebnisses oder das Versenden einer Email nach Fertigstellung der Aufgabe. Wenn Sie keine Option auswählen, wird für das entsprechende Ergebnis keine Aktion vorgenommen.

Auf der Registerkarte **Trace** können Sie ein Trace für einen bestimmten Treiber konfigurieren. Weitere Informationen finden Sie unter „Trace-Stufe konfigurieren“, auf Seite 175.

Abbildung 23-4 *Erweiterte Einstellungen verwalten*



Protokollierumfang und Trace-Stufe von Treibern konfigurieren

Um den Protokollierumfang und die Trace-Stufe für Ihre Treiber zu konfigurieren, wählen Sie auf der Identity Console-Hauptseite die Registerkarte **Treiber** > **Protokoll- und Trace-Konfiguration** aus. Dieser Abschnitt behandelt die folgenden Themen:

- „Protokollierumfang konfigurieren“, auf Seite 174
- „Trace-Stufe konfigurieren“, auf Seite 175

Protokollierumfang konfigurieren

Jeder Treiber hat ein Feld „Protokollierumfang“, über das Sie festlegen können, in welchem Umfang Fehler protokolliert werden sollen. Die hier angegebene Stufe bestimmt, welche Meldungen in den Protokollen verfügbar sind. Standardmäßig ist der Protokollierumfang auf Fehlermeldungen eingeschränkt (dazu gehören auch schwerwiegende Fehler). Um zusätzliche Nachrichtentypen nachzuverfolgen, ändern Sie den Protokollierumfang. Um den Protokollierumfang zu konfigurieren, wählen Sie die Registerkarte **Protokoll- und Trace-Konfiguration** > **Protokollierumfang** aus. Die folgende Tabelle beschreibt die Einstellungen für den Protokollierumfang:

Option	Beschreibung
Protokolleinstellungen vom Treibersatz verwenden	Wenn diese Option ausgewählt ist, protokolliert der Treiber Ereignisse basierend auf den Protokolleinstellungen des Treibersatzobjekts.
Protokollierung in Treibersatz-, Abonnenten- und Herausgeberprotokolle ausschalten	Diese Option deaktiviert die gesamte Protokollierung für diesen Treiber im Treibersatzobjekt, im Abonnentenkanal und im Herausgeberkanal.

Option	Beschreibung
Höchstanzahl an Einträgen im Protokoll (50–500)	Anzahl der Einträge im Protokoll. Der Standardwert ist 50.
Protokollierumfang	Die folgenden Einstellungen stehen für den Protokollierumfang zur Auswahl: ◆ **Fehler protokollieren**: Nur Fehler werden protokolliert. ◆ Fehler und Warnungen protokollieren: Fehler und Warnmeldungen werden protokolliert. ◆ **Spezifische Ereignisse protokollieren**: Die ausgewählten Ereignisse werden protokolliert. Wenn Sie diese Option auswählen, wird die folgende Liste von Ereignissen aktiviert: ◆ **Metadirectory-Engine-Ereignisse** ◆ **Statusereignisse** ◆ **Vorgangsereignisse** ◆ **Transformationsereignisse** ◆ **Berechtigungsbereitstellungsereignisse** ◆ **Nur letzte Protokollierungszeit aktualisieren**: Die letzte Protokollierungszeit wird aktualisiert. ◆ **Protokollierung deaktiviert**: Die Protokollierung wird für den Treiber deaktiviert.

Trace-Stufe konfigurieren

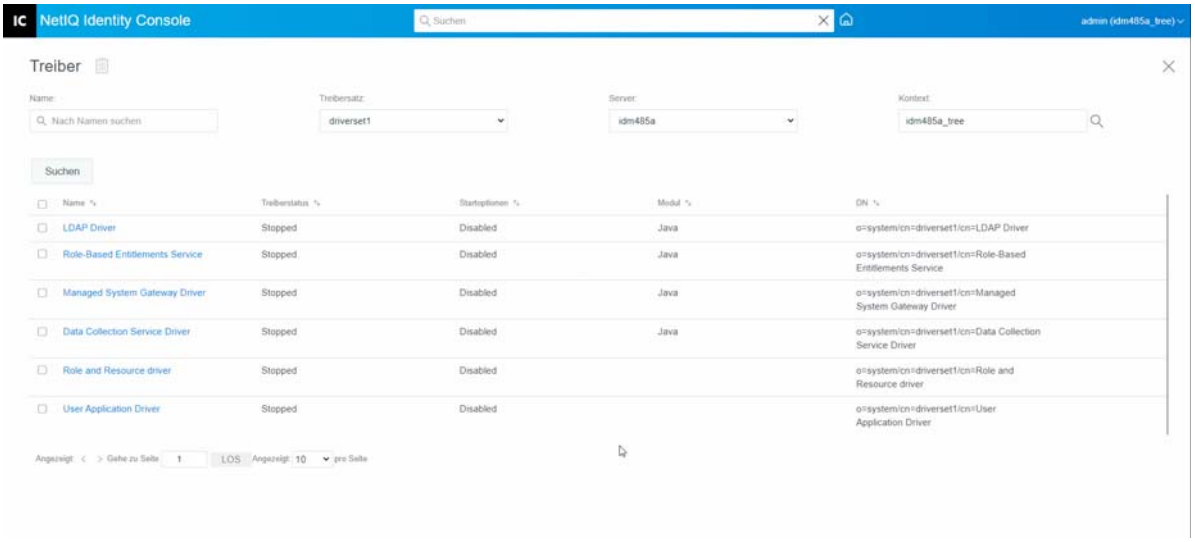
Sie können die Trace-Stufe für einen bestimmten Treiber konfigurieren. Je nach der für einen bestimmten Treiber festgelegten Trace-Stufe werden im Trace treiberbezogene Ereignisse angezeigt, wenn die Engine die Ereignisse verarbeitet. Die Treiber-Trace-Stufe gilt nur für den Treiber oder Treibersatz, für den das Trace festgelegt ist. Wenn Sie Remote Loader verwenden, wird die Remote Loader-Trace-Datei direkt auf Remote Loader festgelegt und enthält nur das Treiber-Shim-Trace.

Um die Trace-Stufe für einen Treiber zu konfigurieren, wählen Sie die Registerkarte **Protokoll- und Trace-Konfiguration** > **Trace** aus. Die folgende Tabelle beschreibt die Trace-Einstellungen:

Parameter	Treiber
Trace-Stufe	Je höher die Treiber-Trace-Stufe, desto mehr Informationen werden im Trace angezeigt. Trace-Stufe 1 zeigt Fehler, aber nicht die Ursache für die Fehler an. Wenn Sie Informationen zur Passwortsynchronisierung anzeigen möchten, setzen Sie die Trace-Stufe auf 5. Wenn Sie **Einstellungen aus dem Treibersatz verwenden** auswählen, wird der Wert vom Treibersatz übernommen.

Parameter	Treiber
Trace-Datei	Geben Sie den Namen und Speicherort einer Datei an, in die die Identity Manager-Informationen für den ausgewählten Treiber geschrieben werden. Wenn Sie **Einstellungen aus dem Treibersatz verwenden** auswählen, wird der Wert vom Treibersatz übernommen.
Trace-Name	Anstelle des Treibernamens wird Treiber-Trace-Meldungen der eingegebene Wert vorangestellt. Verwenden Sie diesen Parameter, wenn der Treibername sehr lang ist.
Kodierung der Trace-Datei	Die Trace-Datei verwendet die Standardkodierung des Systems. Sie können bei Bedarf eine andere Kodierung angeben.
Größenlimit der Trace-Datei	Ermöglicht Ihnen das Festlegen eines Größenlimits für die Java-Trace-Datei. Wenn Sie die Dateigröße auf „Unbegrenzt“ setzen, nimmt die Datei so lange an Größe zu, bis kein Festplattenplatz mehr vorhanden ist. **HINWEIS:** Wenn eine Dateigrößenbeschränkung angegeben wird, wird die Trace-Datei in mehreren Dateien erstellt. Identity Manager teilt automatisch die maximale Dateigröße durch zehn und erstellt zehn separate Dateien. Die kombinierte Größe dieser Dateien entspricht der maximalen Größe der Trace-Datei. Wenn Sie **Einstellungen aus dem Treibersatz verwenden** auswählen, wird der Wert vom Treibersatz übernommen.

Abbildung 23-5 *Protokollierumfang und Trace-Stufe von Treibern verwalten*



Treiber untersuchen

Mit dem Treiberinspektor können Sie detaillierte Informationen zu den Objekten anzeigen, die mit einem Treiber verknüpft sind. Dieser Abschnitt behandelt die folgenden Themen:

Treiberinspektor

So zeigen Sie die mit einem Treiber verknüpften Objekte an:

1. Wählen Sie in Identity Console die Registerkarte **Treiber** > **Inspektor** > **Treiberinspektor** aus.
2. Geben Sie im Feld **Treiber** den vollständigen eindeutigen Namen des Treibers an, den Sie untersuchen möchten, oder klicken Sie auf das Symbol „Durchsuchen“, um den gewünschten Treiber durch Durchsuchen auszuwählen.
3. Nachdem Sie den zu untersuchenden Treiber ausgewählt haben, klicken Sie auf **OK**, um die Seite „Treiberinspektor“ anzuzeigen.

   Auf der Seite werden Informationen über die mit dem ausgewählten Treiber verknüpften Objekte angezeigt. Sie können beliebige der folgenden Aktionen ausführen:

   - **Löschen:** Entfernt die Verknüpfung zwischen dem Treiber und einem Objekt. Aktivieren Sie das Kontrollkästchen vor dem Objekt, das nicht mehr mit dem Treiber verknüpft sein soll, klicken Sie auf das Symbol  und klicken Sie dann zum Bestätigen des Löschens auf **OK**.
   - **Aktualisieren:** Mit dem Aktualisierungssymbol  können Sie alle mit dem Treiber verknüpften Objekte erneut lesen und die angezeigten Informationen aktualisieren.
   - **Anzeigen:** Wählen Sie aus, wie viele Verknüpfungen pro Seite angezeigt werden sollen. Sie können eine vordefinierte Anzahl (25, 50 oder 100) auswählen oder eine beliebige andere Anzahl angeben. Die Standardeinstellung ist 10 Verknüpfungen pro Seite. Wenn mehr Verknüpfungen als die angezeigte Anzahl vorhanden sind, können Sie mithilfe der Pfeilschaltflächen die nächste bzw. vorherige Seite mit Verknüpfungen anzeigen.
   - **Aktionen:** Führen Sie Aktionen für die mit dem Treiber verknüpften Objekte aus. Klicken Sie auf **Aktionen** und wählen Sie dann eine der folgenden Optionen aus:
     - **Alle Verknüpfungen anzeigen:** Zeigt alle mit dem Treiber verknüpften Objekte an.
     - **Nach Verknüpfungen mit Status 'Deaktiviert' filtern:** Zeigt alle mit dem Treiber verknüpften Objekte an, die den Status „Deaktiviert“ haben.
     - **Nach Verknüpfungen vom Typ 'Manuell' filtern:** Zeigt alle mit dem Treiber verknüpften Objekte an, die den Status „Manuell“ haben.
     - **Nach Verknüpfungen vom Typ 'Migrieren' filtern:** Zeigt alle mit dem Treiber verknüpften Objekte an, die den Status „Migrieren“ haben.
     - **Nach Verknüpfungen mit Status 'Ausstehend' filtern:** Zeigt alle mit dem Treiber verknüpften Objekte an, die den Status „Ausstehend“ haben.

- **Nach Verknüpfungen mit Status 'Verarbeitet' filtern:** Zeigt alle mit dem Treiber verknüpften Objekte an, die den Status „Verarbeitet“ haben.
- **Nach Verknüpfungen mit Status 'Nicht definiert' filtern:** Zeigt alle mit dem Treiber verknüpften Objekte an, die den Status „Nicht definiert“ haben.
- **Verknüpfungszusammenfassung:** Zeigt den Status aller mit dem Treiber verknüpften Objekte an.

- **Objekt-DN:** Zeigt den DN der verknüpften Objekte an.
- **Status:** Zeigt den Verknüpfungsstatus des Objekts an.
- **Objektname:** Zeigt den Wert der Verknüpfung an.

Treiber-Cache-Inspektor

In Identity Console können Sie die Transaktionen in der Cache-Datei eines Treibers anzeigen. Der **Treiber-Cache-Inspektor** zeigt Informationen zur Cache-Datei an, einschließlich einer Liste der vom Treiber zu verarbeitenden Ereignisse.

1. Wählen Sie in Identity Console die Registerkarte **Treiber** > **Inspektor** > **Treiber-Cache-Inspektor** aus.
2. Geben Sie im Feld **Treiber** den vollständigen eindeutigen Namen des Treibers an, dessen Cache Sie untersuchen möchten, oder klicken Sie auf das Symbol zum Durchsuchen, um den gewünschten Treiber durch Durchsuchen auszuwählen, und klicken Sie dann auf **OK**, um die Seite „Treiber-Cache-Inspektor“ anzuzeigen.

   Die Cache-Datei eines Treibers kann schreibgeschützt sein, während der Treiber nicht ausgeführt wird. Wenn der Treiber gestoppt ist, wird auf der Seite „Treiber-Cache-Inspektor“ der Cache angezeigt. Wenn der Treiber ausgeführt wird, wird auf der Seite anstelle der Cache-Einträge der Hinweis `Treiber ist nicht gestoppt, Lesen des Cache nicht möglich` angezeigt. Um den Treiber zu stoppen, klicken Sie auf die Schaltfläche  ; der Cache wird dann gelesen und angezeigt.

   - **Treiber-Cache auf Server:** Listet den Server auf, der diese Instanz der Cache-Datei enthält. Wenn der Treiber auf mehreren Servern ausgeführt wird, können Sie einen anderen Server in der Liste auswählen, um die Cache-Datei des Treibers für diesen Server anzuzeigen.
   - **Symbole „Treiber starten“ und „Treiber stoppen“:** Zeigt den aktuellen Status des Treibers an und ermöglicht das Starten oder Stoppen des Treibers. Der Cache kann nur gelesen werden, während der Treiber gestoppt ist.
   - **Löschen:** Wählen Sie Einträge im Cache aus und klicken Sie dann auf das Symbol  , um sie aus der Cache-Datei zu entfernen.
   - **Aktionen:** Ermöglicht das Ausführen von Aktionen für die Einträge in der Cache-Datei. Klicken Sie auf **Aktionen**, um das Menü zu erweitern, und wählen Sie eine der folgenden Optionen aus:
     - **Alle im Cache gespeicherten Ereignisse löschen:** Bietet die Möglichkeit, alle im Cache gespeicherten Ereignisse zu löschen.
     - **Cache-Übersicht:** Zeigt eine Übersicht aller in der Cache-Datei gespeicherten Ereignisse an.

Details des verbundenen Systems für Treiber anzeigen

Führen Sie die folgenden Aktionen aus, um die Details des verbundenen Systems für einen bestimmten Treiber anzuzeigen:

1. Klicken Sie in Identity Console auf das Modul **Objektinspektor**.
2. Wählen Sie durch Durchsuchen das spezifische Treiberobjekt aus, für das Sie die verbundenen Systeme anzeigen möchten.
3. Alle Details zu verbundenen Systemen des ausgewählten Treiberobjekts werden auf Ihrem Computer angezeigt.

Inspektor für Out-of-Band-Synchronisierungs-Cache

So zeigen Sie Ereignisse im Out-of-Band-Synchronisierungs-Cache an:

1. Wählen Sie in Identity Console die Registerkarte **Treiber** > **Inspektor** > **Inspektor für Out-of-Band-Synchronisierungs-Cache** aus.
2. Geben Sie im Feld **Treiber** den vollständigen eindeutigen Namen des Treibers an, dessen Cache Sie untersuchen möchten, oder klicken Sie auf das Symbol „Durchsuchen“, um den gewünschten Treiber durch Durchsuchen auszuwählen. Klicken Sie dann auf **OK**.

   Die Cache-Datei eines Treibers kann schreibgeschützt sein, während der Treiber nicht ausgeführt wird. Wenn der Treiber gestoppt ist, wird auf der Seite „Treiber-Cache-Inspektor“ der Cache angezeigt. Wenn der Treiber ausgeführt wird, wird auf der Seite anstelle der Cache-Einträge der Hinweis `Treiber ist nicht gestoppt, Lesen des Cache nicht möglich` angezeigt. Um den Treiber zu stoppen, klicken Sie auf die Schaltfläche  ; der Cache wird dann gelesen und angezeigt.

   - **Cache-Dateiname:** Zeigt den Dateinamen des Cache an.
   - **Treiber-Cache auf Server:** Listet den Server auf, der diese Instanz der Cache-Datei enthält. Wenn der Treiber auf mehreren Servern ausgeführt wird, können Sie einen anderen Server in der Liste auswählen, um die Cache-Datei des Treibers für diesen Server anzuzeigen.
   - **Symbole „Treiber starten“ und „Treiber stoppen“:** Zeigt den aktuellen Status des Treibers an und ermöglicht das Starten oder Stoppen des Treibers. Der Cache kann nur gelesen werden, während der Treiber gestoppt ist.
   - **Löschen:** Wählen Sie Einträge im Cache aus und klicken Sie dann auf das Symbol  , um sie aus der Cache-Datei zu entfernen.
   - **Aktionen:** Ermöglicht das Ausführen von Aktionen für die Einträge in der Cache-Datei. Klicken Sie auf **Aktionen**, um das Menü zu erweitern, und wählen Sie eine der folgenden Optionen aus:
     - **Cache-Übersicht:** Zeigt eine Übersicht aller in der Cache-Datei gespeicherten Ereignisse an.
     - **Alle im Cache gespeicherten Ereignisse löschen:** Bietet die Möglichkeit, alle im Cache gespeicherten Ereignisse zu löschen.

Treibermanifest

Das Treibermanifest ist eine Art Zusammenfassung des Treibers. Es gibt an, was der Treiber unterstützt und enthält einige Konfigurationseinstellungen. Das Treibermanifest sollte vom Entwickler des Treibers zur Verfügung gestellt werden. Eine Bearbeitung des Treibermanifests durch den Netzwerkadministrator ist in der Regel nicht erforderlich. Falls der Administrator das Treibermanifest bearbeiten möchte, hierzu **Treiber** > **Inspektor** > **Treibermanifest** > **Enable XML Editing** (XML-Bearbeitung aktivieren) auswählen.

Treiberzustand überwachen

Mithilfe der Treiberzustandsüberwachung können Sie den aktuellen Zustand des Treibers durch einen grünen, gelben oder roten Indikator anzeigen und die Aktionen definieren, die für den jeweiligen Zustand ausgeführt werden sollen.

Sie erstellen die Bedingungen (Kriterien), nach denen die einzelnen Zustände ermittelt werden, und definieren die Aktionen, die ausgeführt werden sollen, wenn sich der Zustand des Treibers ändert. Wenn der Treiberzustand beispielsweise vom grünen Zustand in den gelben Zustand wechselt, können Aktionen wie ein Neustart oder das Herunterfahren des Treibers oder der Versand einer Email an die bei Treiberproblemen zuständige Person ausgeführt werden.

Mit diesem Modul können Sie die folgenden Aufgaben ausführen:

- „Treiberzustandsbedingungen ändern“, auf Seite 180
- „Treiberzustandsaktionen ändern“, auf Seite 183
- „Benutzerdefinierten Status erstellen“, auf Seite 185
- „Benutzerdefinierten Status ändern“, auf Seite 185

Treiberzustandsbedingungen ändern

Sie legen die Bedingungen fest, die die einzelnen Treiberzustände bestimmen. Der grüne Zustand soll einen ordnungsgemäßen Treiber repräsentieren, der rote einen nicht ordnungsgemäßen Treiber.

Die Bedingungen für den grünen Zustand werden zuerst ausgewertet. Wenn der Treiber diese Bedingungen nicht erfüllt, werden die Bedingungen für den gelben Zustand ausgewertet. Wenn der Treiber diese Bedingungen ebenfalls nicht erfüllt, wird ihm automatisch der rote Zustand zugewiesen.

So ändern Sie die Bedingungen für einen Zustand:

1. Öffnen Sie in Identity Console die Seite „Treiberzustandskonfiguration“ für einen Treiber, dessen Bedingungen Sie ändern möchten:
   - **1a** Öffnen Sie die Identity Console-Startseite.
   - **1b** Wählen Sie **Treiber** aus und klicken Sie in der Liste auf den gewünschten Treiber. Wählen Sie dann **Inspektor** > **Treiberzustandskonfiguration** aus.
2. Klicken Sie auf die Registerkarte für den Zustand, den Sie ändern möchten (grün oder gelb).

   Die Registerkarte zeigt die aktuellen Bedingungen für den Zustand an. Bedingungen werden in Gruppen unterteilt, und die Bedingungen und die Gruppen werden mithilfe der logischen Operatoren UND und ODER kombiniert. Nachfolgend sehen Sie ein Beispiel für den grünen Zustand:

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

In dem Beispiel wird dem Treiber der grüne Zustand zugewiesen, wenn entweder die Bedingungen von GRUPPE1 oder die Bedingungen von GRUPPE2 als "Wahr" ausgewertet werden. Wenn keine der Bedingungsgruppen als "Wahr" ausgewertet wird, werden die Bedingungen für den gelben Zustand ausgewertet.

Die folgenden Bedingungen können ausgewertet werden:

- **Treiberstatus:** „wird ausgeführt“, „gestoppt“, „wird gestartet“, „wird nicht ausgeführt“ oder „wird heruntergefahren“. Beispielsweise ist eine der Standardbedingungen für den grünen Zustand, dass der Treiber ausgeführt wird.
- **Treiber im Cache-Überlauf:** Der Status des Cache, der zum Speichern von Treibertransaktionen verwendet wird. Wenn sich der Treiber im Cache-Überlauf befindet, wurde der gesamte verfügbare Cache verwendet. Beispielsweise ist die Standardbedingung für den grünen Zustand, dass die Bedingung „Treiber im Cache-Überlauf“ nicht erfüllt (falsch) ist, und die Standardbedingung für den gelben Zustand ist, dass die Bedingung „Treiber in Cache-Überlauf“ erfüllt (wahr) ist.
- **Neueste:** Das Alter der neuesten Transaktion im Cache.
- **Älteste:** Das Alter der ältesten Transaktion im Cache.
- **Gesamtgröße:** Die Größe des Cache.
- **Nicht verarbeitete Größe:** Die Größe aller nicht verarbeiteten Transaktionen im Cache.
- **Nicht verarbeitete Transaktionen:** Die Anzahl der nicht verarbeiteten Transaktionen im Cache. Sie können alle Transaktionstypen oder bestimmte Transaktionstypen angeben (z. B. Hinzufügungen, Entfernungen oder Umbenennungen).
- **Transaktionsverlauf:** Die Anzahl der in einem bestimmten Zeitraum an verschiedenen Punkten im Abonnenten- oder Herausgeberkanal verarbeiteten Transaktionen. Diese Bedingung verwendet mehrere Elemente im folgenden Format:

  <*Transaktionstyp*> <*Transaktionsort und -zeitraum*> <*relationaler Operator*> <*Transaktionsanzahl*>.

  - <*Transaktionstyp*>: Gibt den Typ der Transaktion an, die ausgewertet wird. Dabei kann es sich um alle Transaktionen handeln, Hinzufügungen, Entfernungen, Umbenennungen usw.
  - <*Transaktionsort und -zeitraum*>: Gibt den Ort im Abonnenten- oder Herausgeberkanal und den Zeitraum an, der ausgewertet wird. Beispielsweise können Sie die Gesamtanzahl der Transaktionen auswerten, die in den letzten 48 Stunden als vom Herausgeber berichtete Ereignisse verarbeitet wurden. Standardmäßig werden die Daten im Transaktionsverlauf zwei Wochen beibehalten. Dies bedeutet, dass Sie nur dann einen längeren Zeitraum als zwei Wochen angeben können, wenn Sie die standardmäßige Einstellung für die Datenbeibehaltungsdauer des Transaktionsverlaufs ändern.

- <*relationaler Operator*>: Gibt an, dass die identifizierten Transaktionen entweder gleich, ungleich, kleiner als, kleiner gleich, größer als oder größer gleich der <Transaktionsanzahl> sein müssen.
- <*Transaktionsanzahl*>: Gibt die Anzahl der Transaktionen an, die in der Auswertung verwendet werden.

Nachfolgend sehen Sie ein Beispiel für eine Transaktionshistorien-Bedingung:

```
<Anzahl der Hinzufügungen> <als Herausgeberbefehle> <in den letzten 10 Minuten> <ist kleiner als> <1000>
```

- **Verfügbarer Verlauf:** Die Menge der Transaktionsverlaufsdaten, die zur Auswertung zur Verfügung steht. Der Hauptzweck dieser Bedingung besteht darin, zu verhindern, dass eine Transaktionshistorienbedingung zum Fehlschlagen des aktuellen Zustands führt, weil für den ausgewerteten Zeitraum nicht genügend Transaktionshistoriendaten gesammelt wurden.

  Nehmen Sie beispielsweise an, dass Sie die Transaktionsverlaufsbedingung dazu verwenden möchten, die Anzahl der Hinzufügungen als Herausgeberbefehle in den letzten 48 Stunden auszuwerten (wie in dem Beispiel im obenstehenden Abschnitt „Transaktionsverlauf“). Sie möchten jedoch verhindern, dass die Bedingung fehlschlägt, wenn nur für einen kürzeren Zeitraum als 48 Stunden Daten vorliegen. Dies kann nach der anfänglichen Einrichtung der Zustandskonfiguration des Treibers oder bei einem Neustart des Treiber-Servers der Fall sein (die Transaktionshistoriendaten werden im Arbeitsspeicher aufbewahrt). Daher können Sie Bedingungsgruppen wie die folgenden erstellen:

  ```
  Gruppe1 Verfügbarer Verlauf <ist kleiner als> <48 Stunden> oder
  Group2 Verfügbarer Verlauf <ist größer oder gleich> <48 Stunden> und
  Transaktionsverlauf <Anzahl der Hinzufügungen> <als
  Herausgeberbefehle> <in den letzten 48 Stunden> <ist kleiner als>
  <1000>
  ```

  Der Zustand wird als „wahr“ ausgewertet, wenn eine der Bedingungsgruppen wahr ist, d. h. wenn a) Daten aus weniger als 48 Stunden vorliegen oder b) Daten aus mindestens 48 Stunden vorliegen und die Anzahl der Hinzufügungen als Herausgeberbefehle in den letzten 48 Stunden kleiner als 1000 ist.

  Der Zustand wird als "Falsch" ausgewertet, wenn beide Bedingungen als "Falsch" ausgewertet werden, d. h. wenn a) Daten aus mindestens 48 Stunden vorliegen und b) die Anzahl der Hinzufügungen als Herausgeber-Befehle in den letzten 48 Stunden größer ist als 1000.

3 Bearbeiten Sie die Kriterien nach Bedarf.

- Um eine neue Gruppe hinzuzufügen, klicken Sie auf das Symbol + neben den **Bedingungsgruppen**.
- Um eine Bedingung hinzuzufügen, klicken Sie auf das Symbol + neben den logischen Operatoren (UND/ODER). Alternativ können Sie auch auf den Link **Neue Bedingung hinzufügen** klicken.
- Sie können Bedingungsgruppen oder einzelne Bedingungen neu anordnen, indem Sie das Kontrollkästchen vor der Gruppe oder Bedingung auswählen, die Sie verschieben möchten, und anschließend auf die Pfeilschaltflächen klicken, um sie nach oben oder unten zu verschieben. Mit den Pfeilschaltflächen können Sie auch eine Bedingung von einer Gruppe in eine andere verschieben.

4 Wenn Sie fertig sind, speichern Sie Ihre Änderungen, indem Sie auf die Schaltfläche **Speichern** klicken.

5 Wenn Sie die Aktionen ändern möchten, die mit den festgelegten Bedingungen verknüpft sind, fahren Sie mit „Treiberzustandsaktionen ändern“, auf Seite 183 fort.

Treiberzustandsaktionen ändern

Sie können festlegen, welche Aktionen ausgeführt werden sollen, wenn sich der Treiberzustand ändert. Wenn sich der Zustand von grün in gelb ändert, können Sie den Treiber herunterfahren oder neu starten, ein Ereignis generieren oder einen Workflow starten. Wenn sich der Zustand von gelb in grün ändert, können beliebige mit dem grünen Zustand verknüpfte Aktionen ausgeführt werden.

Die Aktionen eines Zustands werden nur einmal ausgeführt, wenn die Bedingungen erfüllt sind. Solange die Bedingung wahr bzw. der Zustand unverändert bleibt, werden die Aktionen nicht wiederholt. Wenn sich der Zustand ändert, weil seine Bedingungen nicht länger erfüllt sind, werden die Aktionen beim nächsten Mal, wenn die Bedingungen wieder erfüllt sind, erneut ausgeführt.

1 Öffnen Sie in Identity Console die Seite „Treiberzustandskonfiguration“ für einen Treiber, dessen Aktionen Sie ändern möchten:

   1a Öffnen Sie die Identity Console-Startseite.

   1b Wählen Sie **Treiber** aus und klicken Sie in der Liste auf den gewünschten Treiber. Wählen Sie dann **Inspektor** > **Treiberzustandskonfiguration** aus.

2 Klicken Sie auf die entsprechende Registerkarte **Grün**, **Gelb** oder **Rot** für den Zustand, dessen Aktionen Sie ändern möchten.

3 Klicken Sie auf das Plussymbol (+) neben der Überschrift **Aktionen**, um eine Aktion hinzuzufügen, und wählen Sie dann den gewünschten Aktionstyp aus:

   - **Start driver:** Startet den Treiber.
   - **Stop driver:** Stoppt den Treiber.
   - **Treiber neu starten:** Stoppt den Treiber und startet ihn anschließend.
   - **Treiber-Cache löschen:** Entfernt alle Transaktionen, einschließlich nicht verarbeiteter Transaktionen, aus dem Cache.
   - **Email senden:** Sendet einem oder mehreren Empfängern eine Email. Die Schablone, die Sie für den Email-Nachrichtentext verwenden möchten, muss bereits vorhanden sein. Wenn Sie den Treibernamen, den Servernamen und Informationen zum aktuellen Treiberzustand in die Email einfügen möchten, fügen Sie die Token `$Driver$`, `$Server$` und `$HealthState$` zur Email-Schablone hinzu und fügen Sie die Token dann in den Nachrichtentext ein. Beispiel:

     ```
     The current health state of the $Driver$ driver running on $Server$ is $HealthState$.
     ```

     WICHTIG: Um Emails an mehrere Benutzer zu senden, trennen Sie jede Email-Adresse nur durch ein Komma (,). Verwenden Sie kein Semikolons anstelle von Kommas.

   - **Trace-Nachricht schreiben:** Schreibt eine Nachricht in die Protokolldatei des Treiberzustandsauftrags oder die Protokolldatei des Treibersatzes, wenn die Trace-Datei nicht für den Treiberzustandsauftrag konfiguriert ist.

- **Ereignis generieren:** Generiert ein Ereignis, das von Audit und Sentinel verwendet werden kann.
- **ECMA-Skript ausführen:** Führt ein vorhandenes ECMA-Skript aus.

  Informationen zum Bilden von ECMA-Skripten finden Sie unter Using ECMAScript in Policies (ECMA-Skript in Richtlinien verwenden) in *NetIQ Identity Manager - Using Designer to Create Policies* (NetIQ Identity Manager – Richtlinien mit Designer erstellen).
- **Workflow starten:** Startet einen Bereitstellungsworkflow.
- **Bei Fehler:** Gibt an, was im Falle eines Fehlers bei einer Aktion mit den verbleibenden Aktionen, dem aktuellen Treiberzustand und dem Treiberzustandsauftrag geschehen soll.
  - **Auswirkung auf Aktionen:** Sie können die verbleibenden Aktionen weiter ausführen, die Ausführung stoppen oder die aktuelle Einstellung als Standardeinstellung übernehmen. Die aktuelle Einstellung gilt nur dann, wenn mehrere Bei Fehler-Aktionen vorhanden sind und Sie die Option Aktionen betroffen von in einer der vorausgehenden Bei Fehler-Aktionen festlegen.
  - **Auswirkung auf Status:** Sie können den aktuellen Zustand speichern, ihn ablehnen oder die aktuelle Einstellung als Standardeinstellung übernehmen. Wenn Sie den Zustand speichern, werden dessen Bedingungen weiterhin als „wahr“ ausgewertet. Wenn Sie den Zustand ablehnen, werden dessen Bedingungen als „falsch“ ausgewertet. Die aktuelle Einstellung gilt nur dann, wenn mehrere Bei Fehler-Aktionen vorhanden sind und Sie die Option Status betroffen von in einer der vorausgehenden Bei Fehler-Aktionen festlegen.
  - **Auswirkung auf Treiberzustandsauftrag:** Sie können den Auftrag weiterhin ausführen, ihn abbrechen und deaktivieren oder die aktuelle Einstellung als Standardeinstellung übernehmen. Wenn Sie die Ausführung des Auftrags fortsetzen, wertet der Auftrag die Bedingungen noch aus, um den Zustand des Treibers zu ermitteln, und führt die mit dem Zustand verknüpften Aktionen aus. Wenn Sie den Auftrag abbrechen und deaktivieren, wird die aktuelle Aktivität des Auftrags gestoppt und er wird beendet. Der Auftrag wird erst dann wieder ausgeführt, wenn Sie ihn aktivieren. Die aktuelle Einstellung gilt nur dann, wenn mehrere Bei Fehler-Aktionen vorhanden sind und Sie die Einstellung Treiberzustandsauftrag betroffen von in einer der vorausgehenden Bei Fehler-Aktionen festlegen.

4 Wenn Sie fertig sind, speichern Sie Ihre Änderungen, indem Sie auf die Schaltfläche **Speichern** klicken.

Benutzerdefinierten Status erstellen

Sie können einen oder mehrere benutzerdefinierte Status erstellen, um Aktionen unabhängig vom aktuellen Treiberzustand (grün, gelb, rot) auszuführen. Wenn die Bedingungen für einen benutzerdefinierten Status erfüllt sind, werden die definierten Aktionen unabhängig vom aktuellen Treiberzustand ausgeführt.

Genau wie beim grünen, gelben und roten Treiberzustand werden die einem benutzerdefinierten Status zugewiesenen Aktionen nur einmal ausgeführt, wenn die Bedingungen erfüllt werden; solange der Status gültig (wahr) ist, werden die Aktionen nicht wiederholt. Wenn sich der Zustand ändert, weil seine Bedingungen nicht länger erfüllt sind, werden die Aktionen beim nächsten Mal, wenn die Bedingungen wieder erfüllt sind, erneut ausgeführt.

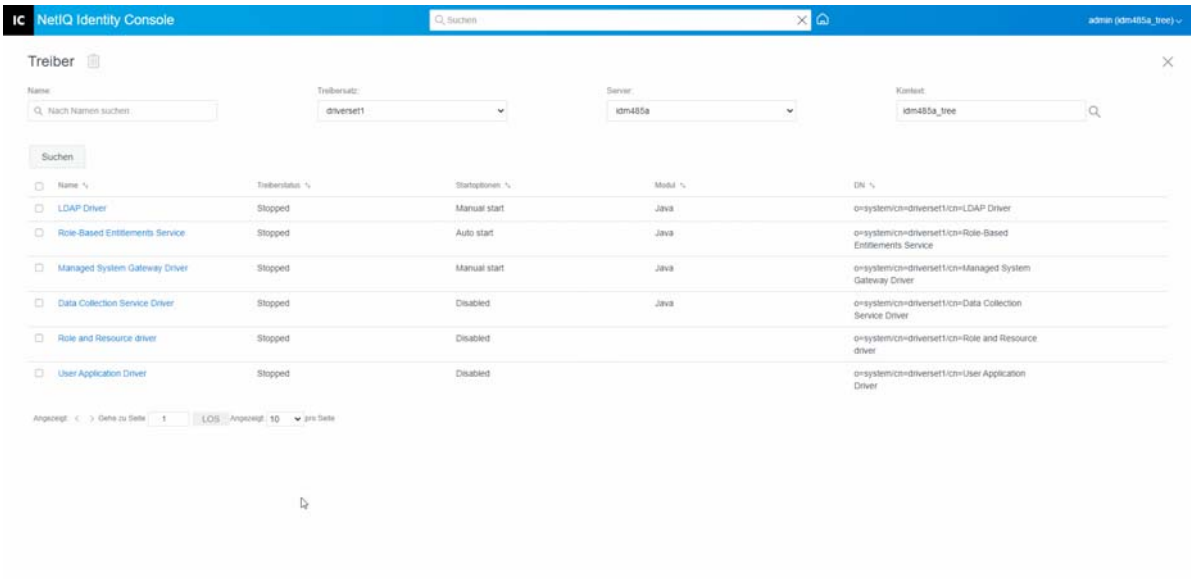
1. Öffnen Sie in Identity Console die Seite „Treiberzustandskonfiguration“ für einen Treiber, für den Sie einen benutzerdefinierten Status erstellen möchten:
   1a. Öffnen Sie die Identity Console-Startseite.
   1b. Wählen Sie **Treiber** aus und klicken Sie in der Liste auf den gewünschten Treiber. Wählen Sie dann **Inspektor** > **Treiberzustandskonfiguration** aus.
2. Klicken Sie auf das Symbol + neben den Treiberzustandssymbolen (grün, gelb und rot).
3. Befolgen Sie die Anweisungen in „Treiberzustandsbedingungen ändern“, auf Seite 180 und „Treiberzustandsaktionen ändern“, auf Seite 183, um die Bedingungen und Aktionen für den benutzerdefinierten Status zu definieren.

Benutzerdefinierten Status ändern

Führen Sie die folgenden Schritte aus, um benutzerdefinierte Status zu ändern:

1. Öffnen Sie in Identity Console die Seite „Treiberzustandskonfiguration“ für einen Treiber, für den Sie einen benutzerdefinierten Status erstellen möchten:
   1a. Öffnen Sie die Identity Console-Startseite.
   1b. Wählen Sie **Treiber** aus und klicken Sie in der Liste auf den gewünschten Treiber. Wählen Sie dann **Inspektor** > **Treiberzustandskonfiguration** aus.
2. Klicken Sie auf das Symbol  neben den Treiberzustandssymbolen (grün, gelb und rot).
3. Befolgen Sie die Anweisungen in „Treiberzustandsbedingungen ändern“, auf Seite 180 und „Treiberzustandsaktionen ändern“, auf Seite 183, um die Bedingungen und Aktionen für den benutzerdefinierten Status zu definieren.

Abbildung 23-6 *Treiberinspektoren verwalten*



24 Treibersatzstatistiken verwalten

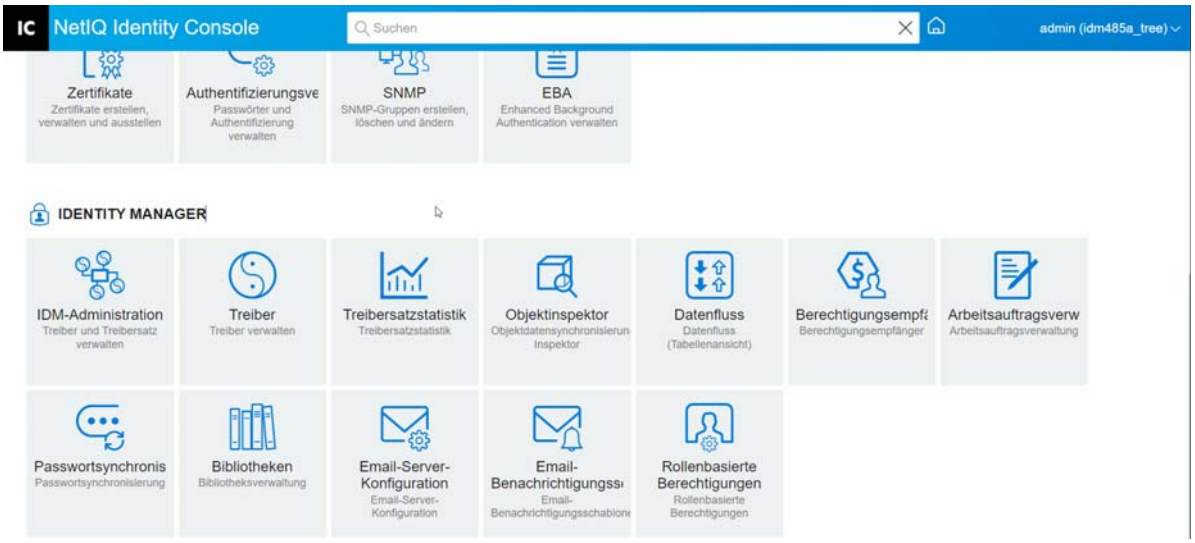
Im Identity Console-Portal können Sie eine Vielzahl von Statistiken für einen einzelnen Treiber oder für einen gesamten Treibersatz anzeigen. Dazu gehören Statistiken wie die Cache-Dateigröße, die Größe der nicht verarbeiteten Transaktionen in der Cache-Datei, die älteste und neueste Transaktion sowie die Gesamtzahl der nicht verarbeiteten Transaktionen nach Kategorie (Hinzufügungen, Entfernungen, Änderungen usw.). So zeigen Sie die Treibersatzstatistiken an:

1. Öffnen Sie in Identity Console die Seite **Treibersatzstatistik**.
2. Wählen Sie in der Dropdown-Liste den gewünschten Server aus.

   Eine Seite wird angezeigt, auf der Sie die Statistik für alle im Treibersatz enthaltenen Treiber anzeigen können.

   - Um die Statistik zu aktualisieren, klicken Sie auf das Symbol .
   - Um die Statistik für einen Treiber zu schließen, klicken Sie auf die Schaltfläche in der oberen rechten Ecke des Statistikfensters des Treibers.
   - Um die Statistik für alle Treiber zu öffnen, klicken Sie auf **Aktionen** > **Alle anzeigen**.
   - Um die Liste der nicht verarbeiteten Transaktionen für einen Treiber zu reduzieren, klicken Sie auf die Schaltfläche oberhalb der Liste. Um die Liste der nicht verarbeiteten Transaktionen für alle Treiber zu reduzieren, klicken Sie auf die Schaltfläche **Aktionen** > **Alle Transaktionen reduzieren**.
   - Um die Liste der Transaktionen zu erweitern, klicken Sie auf die Schaltfläche . Um die Liste der nicht verarbeiteten Transaktionen für alle Treiber zu erweitern, klicken Sie auf **Aktionen** > **Alle Transaktionen erweitern**.
   - Um das Statistik-Dashboard für deaktivierte Treiber zu schließen, klicken Sie auf **Aktionen** und wählen Sie dann **Deaktivierte Treiber ausblenden** aus.

Abbildung 24-1 *Treibersatzstatistiken verwalten*



25 Identity Manager-Objekte untersuchen

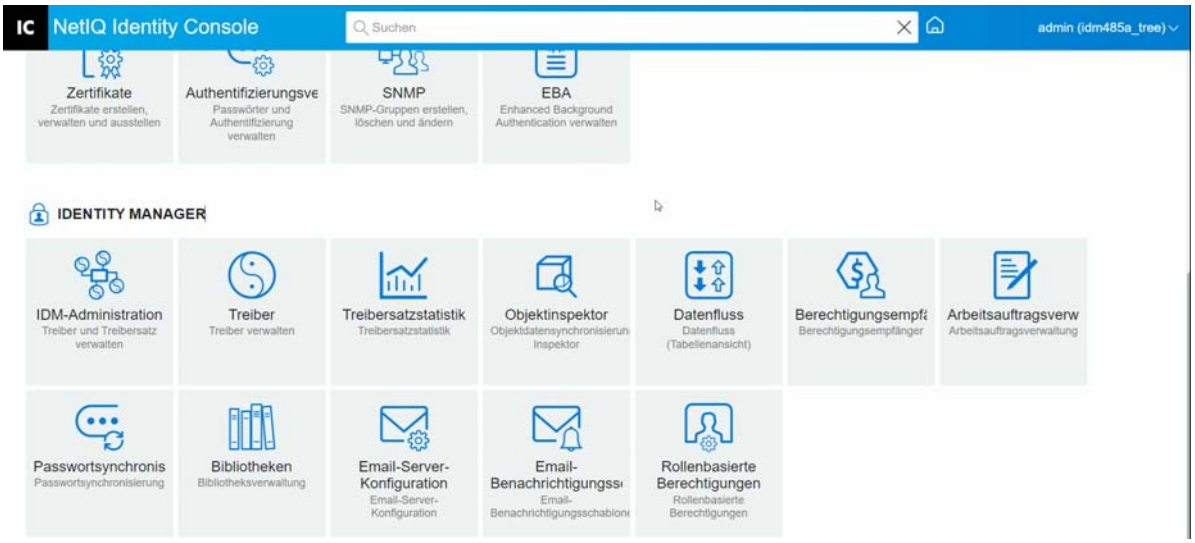
Mit dem Objektinspektor können Sie detaillierte Informationen darüber anzuzeigen, wie ein Objekt an Identity Manager-Beziehungen beteiligt ist. Zu diesen Beziehungen gehören die mit dem Objekt verknüpften verbundenen Systeme, der Datenfluss zwischen dem Identitätsdepot und den verbundenen Systemen, die zurzeit im Identitätsdepot und in den verbundenen Systemen gespeicherten Attributwerte, die Treiberkonfigurationen des verbundenen Systems usw.

Um Identity Manager-Objekte zu untersuchen, klicken Sie auf der Identity Console-Hauptseite auf die Option **Objektinspektor**. Geben Sie den vollständigen eindeutigen Namen des Objekts an, das Sie untersuchen möchten, oder klicken Sie auf das Symbol „Durchsuchen“, um das gewünschte Objekt durch Durchsuchen auszuwählen.

Im Bereich „Verbundene Systeme“ werden die einzelnen verbundenen Systeme aufgeführt, mit denen das Objekt verknüpft ist. Auf der Seite **Objektinspektor** können Sie die folgenden Aktionen ausführen:

- **Verknüpfung hinzufügen**: Um eine neue Verknüpfung zu einem verbundenen System hinzuzufügen, klicken Sie auf das Symbol +. Wählen Sie durch Durchsuchen das **Integrationstreiberobjekt** aus und geben Sie die **Verknüpfte Objekt-ID** an.
- **Verknüpfungen löschen**: Um eine Verknüpfung mit einem verbundenen System zu löschen, aktivieren Sie das Kontrollkästchen links neben der Verknüpfung und klicken Sie auf das Symbol 🗑. Um alle Verknüpfungen zu löschen, aktivieren Sie das Kontrollkästchen unter der Spalte „Löschen“ und klicken Sie dann auf das Symbol 🗑.

Abbildung 25-1 *Identity Manager-Objekte untersuchen*



26 Datenfluss verwalten

Unter „Datenfluss“ werden die Herausgeber- und Abonnentenkanäle für mehrere Treiber in einer einzelnen Ansicht dargestellt. Mit dieser Option können Sie die Dateneigentümerschaft für alle Treiber anzeigen und aktualisieren.

Um auf die Tabellenansicht des Datenflusses zuzugreifen, klicken Sie auf der Identity Console-Hauptseite auf das Modul **Datenfluss (Tabellenansicht)**. Wählen Sie dann durch Durchsuchen den entsprechenden Container aus, um die Liste der Treiber anzuzeigen.

Führen Sie die folgenden Schritte aus, um die Dateneigentümerschaft einzelner Treiber zu verwalten:

1 Jeder Treiber verfügt über zwei Schaltflächen zum Verwalten des Datenflusses in den Herausgeber- und Abonnentenkanälen. Die Schaltfläche auf der linken Seite verwaltet den Datenfluss über den Herausgeberkanal und die Schaltfläche auf der rechten Seite verwaltet den Datenfluss über den Abonnentenkanal.

   1a **Synchronisieren**: Wählen Sie diese Option aus, um das jeweilige Attribut zu synchronisieren. Nach Auswahl dieser Option wechselt das Symbol für den Herausgeberkanal zu ↑ und für den Abonnentenkanal zu ↓.

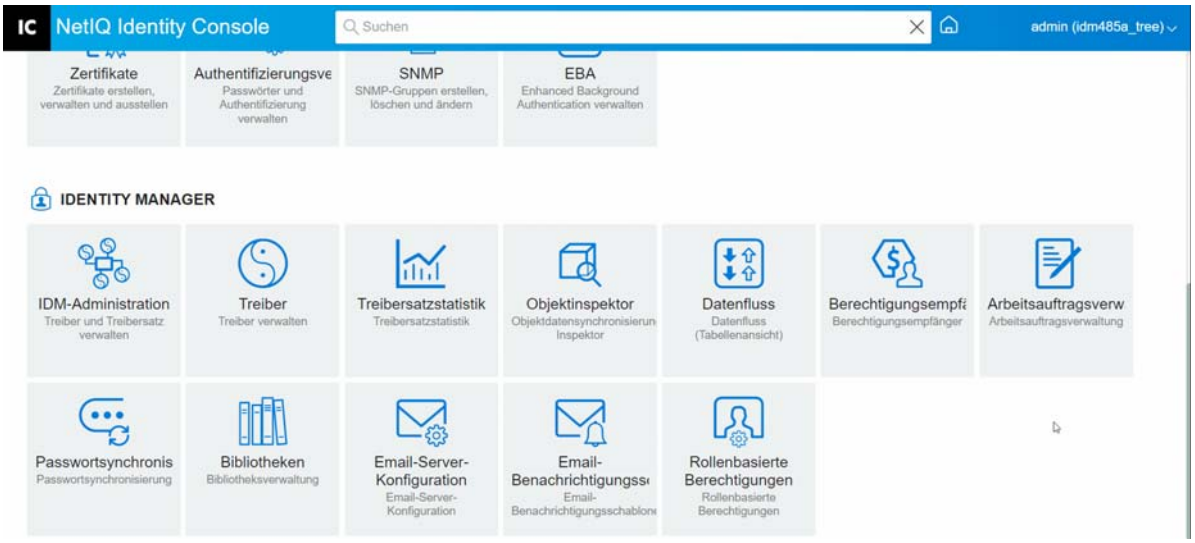
   1b **Ignorieren**: Wählen Sie diese Option aus, um die Synchronisierung des jeweiligen Attributs zu beenden. Das Symbol wechselt nach Auswahl der Option zu ⊘.

   1c **Benachrichtigen**: Wählen Sie diese Option aus, um über Änderungen an einem bestimmten Attribut benachrichtigt zu werden. Die Änderung wird jedoch nicht automatisch synchronisiert. Das Symbol wechselt nach Auswahl der Option zu 🔔.

   1d **Zurücksetzen**: Wählen Sie diese Option aus, um den Attributwert auf den vom anderen Kanal angegebenen Wert zurückzusetzen. Das Symbol wechselt nach Auswahl der Option zu ↻.

   HINWEIS: Sie können diesen Wert für den Herausgeberkanal oder für den Abonnentenkanal festlegen. Es ist jedoch nicht möglich, den Wert für beide Kanäle gleichzeitig festzulegen.

Abbildung 26-1 *Datenfluss verwalten*



27 Berechtigungsempfänger verwalten

Berechtigungsreferenzen und -ergebnisse werden für Objekte gepflegt, für die eine Berechtigung gewährt oder widerrufen wurde. Berechtigungsreferenzen und -ergebnisse enthalten Informationen darüber, ob die Berechtigung für dieses Objekt derzeit gewährt oder widerrufen ist. Berechtigungsempfänger sind alle Objekte, die Bezüge zu einer Berechtigung enthalten.

Berechtigungsreferenzen

Um die Berechtigungsreferenzen und -ergebnisse anzuzeigen, klicken Sie auf der Identity Console-Hauptseite auf die Option **Berechtigungsempfänger** und wählen Sie „Entitlement Reference“ (Berechtigungsreferenz) aus. Geben Sie dann den vollständigen eindeutigen Namen des `DirXML-EntitlementRecipient`-Objekts ein. Sie können auf die Schaltfläche „Objektauswahl“  klicken, um das Objekt auszuwählen.

Berechtigungsergebnisse

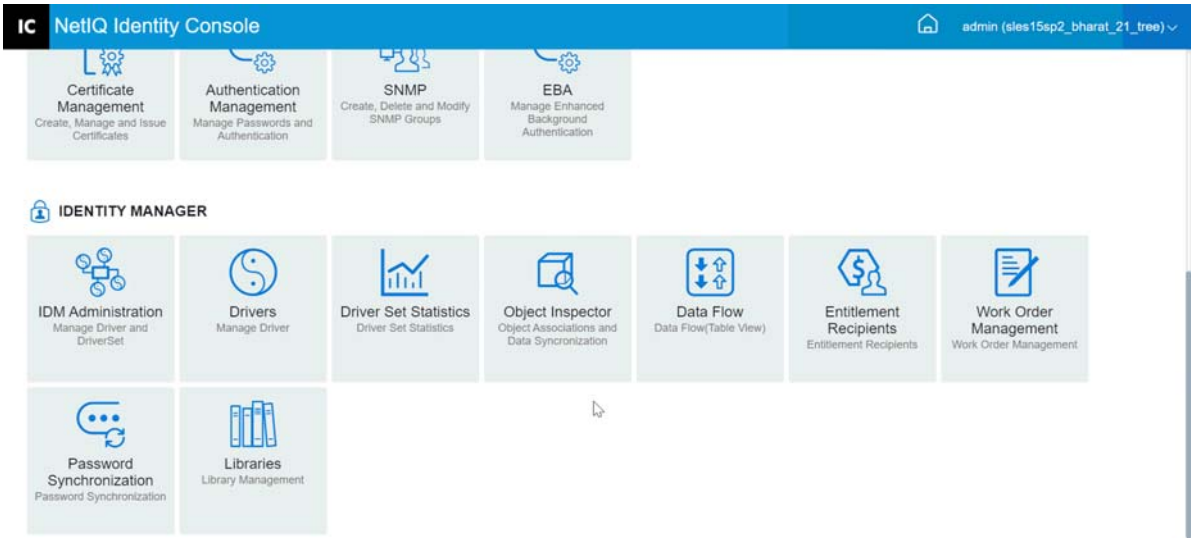
In der Identity Console-Tabelle der Berechtigungsergebnisse werden die mit dem ausgewählten Objekt verknüpften Berechtigungsergebnisse aufgeführt. Wählen Sie zum Anzeigen der zugeordneten Berechtigung deren "Berechtigungs-DN". Wählen Sie zum Anzeigen der Berechtigungsergebnisse im XML-Format die entsprechende Ergebnis-ID.

- **Spaltenüberschriften der Berechtigungsergebnisse**: Die Spaltenüberschriften enthalten folgende Informationen: den vollständigen eindeutigen Namen der Berechtigung, den aktuellen Status („erteilt“ oder „widerrufen“), woher die Ergebnisse stammen (Ursprung), den Status des Ergebnisses, zum Ergebnis gehörende Nachrichten, den Zeitstempel des Ergebnisses und die Identifikation des Ergebnisses.
  - **Berechtigungs-DN**: Klicken Sie auf den eindeutigen Namen (DN) der Berechtigung des Objekts, um die Seite „Objekt ändern“ aufzurufen. Auf dieser Seite können Sie anzeigen, wie eDirectory-Attribute dem Objekt zugewiesen wurden. Außerdem können Sie auf dieser Seite die Attribute des Objekts ändern. Die auf der Seite "Objekt ändern" angezeigte Anzahl der Kategorien hängt von dem ausgewählten Objekt ab.
  - **Status**: Zeigt an, ob die Berechtigung gewährt oder widerrufen wurde. Wenn das Plugin im XML-Stream einen sonstigen Wert findet, wird der entsprechende Wert direkt angezeigt.
  - **Nachricht**: Alle Nachrichten, die das DirXML-Shim mit den Ergebnisstatuswerten verknüpft hat. Die Informationen, die im <msg></msg> Teil der XML-Ergebnisdatei gespeichert sind. Klicken Sie auf den Eintrag "Ergebnis-ID", um die vollständigen Details des Ergebnisses auf einer Seite des XML-Viewers anzuzeigen.

- **Zeitstempel**: Der Zeitpunkt, an dem die Berechtigungs-Engine das Ergebnis verarbeitet und geschrieben hat. Klicken Sie auf den Eintrag "Ergebnis-ID", um die vollständigen Details des Ergebnisses auf einer Seite des XML-Viewers anzuzeigen.
- **Result ID** (Ergebnis-ID): Klicken Sie auf den Eintrag „Result ID“ (Ergebnis-ID), um die vollständigen Details des Ergebnisses auf einer Seite des XML-Viewers anzuzeigen. Klicken Sie auf „Schließen“, wenn Sie mit dem Überprüfen der Ergebnisse fertig sind.

Aktivieren Sie zum Löschen eines Berechtigungsergebnisses das Kontrollkästchen links neben dem Eintrag „Berechtigungsergebnisse“ und klicken Sie anschließend auf **Löschen**.

Abbildung 27-1 *Berechtigungsempfänger verwalten*



28 Arbeitsaufträge verwalten

Identity Manager-Treiber können Arbeitsaufträge als Ergebnis der von den Treibern verarbeiteten Ereignissen erstellen. Wenn Sie beispielsweise einen HR-Treiber (SAP HR, PeopleSoft usw.) verwenden, können Sie festlegen, dass der Treiber bei jedem Hinzufügen eines neuen Benutzers einen Arbeitsauftrag generiert.

Mit Identity Console können Sie Arbeitsaufträge erstellen und verwalten, die für verschiedene Treiber erstellt wurden, die diese spezifische Funktionalität unterstützen.

Neue Arbeitsaufträge erstellen

Führen Sie zum Erstellen eines neuen Arbeitsauftrags die folgenden Schritte aus:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Arbeitsauftrag**.
2. Klicken Sie auf das Symbol +, um einen neuen Arbeitsauftrag zu erstellen.
3. Geben Sie einen Namen für den Arbeitsauftrag ein und klicken Sie anschließend auf **OK**.

   Der Name wird für den Namen des Arbeitsauftragsobjekts im Identitätsdepot verwendet.
4. Füllen Sie die folgenden Felder aus:

   Status: Der Status eines neuen Arbeitsauftrags ist entweder **Ausstehend** oder **Wird gehalten**. In der Regel lautet der Status des Arbeitsauftrags **Ausstehend**. Die Verarbeitung eines Auftrags kann durch Auswahl von**Auf 'Warten' gelegt** gestoppt werden. Nach der Verarbeitung eines Arbeitsauftrags wird der sich ergebende Arbeitsauftragsstatus in diesem Feld angezeigt.

   Fälligkeitsdatum: Sie können festlegen, dass der Treiber den Auftrag sofort ausführen soll, oder Sie können den Auftrag planen. Klicken Sie zum Festlegen eines Fälligkeitsdatums auf das Kalendersymbol. Verwenden Sie zum Auswählen des Datums den Kalender. Wählen Sie den Monat, das Jahr und die Uhrzeit mithilfe der Pfeile aus.

   Wiederholungsauftrag: Wählen Sie diese Option aus, damit der Arbeitsauftrag mehrmals verarbeitet wird. eben Sie das Zeitintervall an, indem Sie auswählen, nach wie vielen Wochen, Tagen, Stunden oder Minuten der Auftrag wiederholt werden soll. Der Arbeitsauftrag wird bis zu seinem Löschdatum wiederholt, sofern er nicht vorher manuell gelöscht oder bearbeitet wurde oder der Treiber eine Fehlermeldung zurückgibt.

   Gelöscht am: Wählen Sie zum Löschen konfigurierter Aufträge ein Datum im Kalender aus. Arbeitsaufträge mit einem Fehlerstatus werden nur gelöscht, wenn Sie **Arbeitsauftrag löschen, selbst wenn der Arbeitsauftrag einen Fehler aufweist** aktivieren.

Abhängige Aufträge: Wenn Sie einen neuen Arbeitsauftrag erstellen, können Sie ihn von einem oder mehreren Arbeitsaufträgen abhängig machen. Klicken Sie auf , um abhängige Arbeitsaufträge durch Durchsuchen auszuwählen. Um einen Arbeitsauftrag aus der Liste zu entfernen, wählen Sie den Arbeitsauftrag aus und klicken Sie dann auf .

Typ: Verwenden Sie dieses Feld, um einen Arbeitsauftragstyp anzugeben. Der Treiber ändert dieses Attribut nicht. Beim Verarbeiten des Arbeitsauftrags wird das Attribut an das WorkToDo-Objekt übergeben.

Auftragsnummer: Eine eindeutige Arbeitsauftragsnummer. Dieser Wert kann von einem anderen Auftragssystem des Unternehmens als NetIQ eDirectory zugewiesen werden, z. B. von einer Arbeitsauftragsdatenbank.

Kontaktangaben: Kontaktinformationen der Person, die für den Auftrag verantwortlich ist.

Auftragsbearbeitungsprotokoll: Nach der Verarbeitung eines Arbeitsauftrags protokolliert der Treiber die Ergebnisse des Arbeitsauftrags einschließlich Status in diesem Feld. Dadurch können Sie den aktuellen Auftragsstatus überprüfen und Probleme identifizieren, die möglicherweise bei der Konfiguration des Auftrags durch den Treiber aufgetreten sind.

Das Statusattribut des Arbeitsauftrags behält den Wert „Ausstehend“, bis der Arbeitsauftrag verarbeitet wurde. Der Arbeitsauftrag wird verarbeitet, wenn das Fälligkeitsdatum abgelaufen ist. Der Treiber meldet die Verarbeitungsergebnisse, indem er das Statusattribut auf "Konfiguriert", "Warnhinweis" oder "Fehler" setzt. Arbeitsaufträge mit dem Status „Wird gehalten“ werden vom Treiber ignoriert.

- **Ausstehend:** Der Treiber wartet auf das Fälligkeitsdatum, um den Arbeitsauftrag zu verarbeiten.
- **Konfiguriert:** Der Arbeitsauftrag wurde erfolgreich verarbeitet.
- **Fehler:** Der Treiber konnte den Arbeitsauftrag nicht ausführen.
- **Warnung:** Für den Arbeitsauftrag ist eine Warnmeldung vorhanden. Wenn ein Arbeitsauftrag beispielsweise einen abhängigen Arbeitsauftrag mit einem späteren Fälligkeitsdatum hat, gibt der Treiber eine Warnmeldung zurück.

Beschreibung: Die Beschreibung des Auftrags.

Arbeitsauftragsinhalt: Die Daten in diesem Feld werden von den Treiberregeln zum Verarbeiten des Arbeitsauftrags verwendet. Es kann sich dabei beispielsweise um XML-Code handeln, der von der Befehlstransformation zum Verarbeiten des Arbeitsauftrags verwendet wird.

Vorhandene Arbeitsaufträge löschen

Führen Sie die folgenden Schritte aus, um einen vorhandenen Arbeitsauftrag zu löschen:

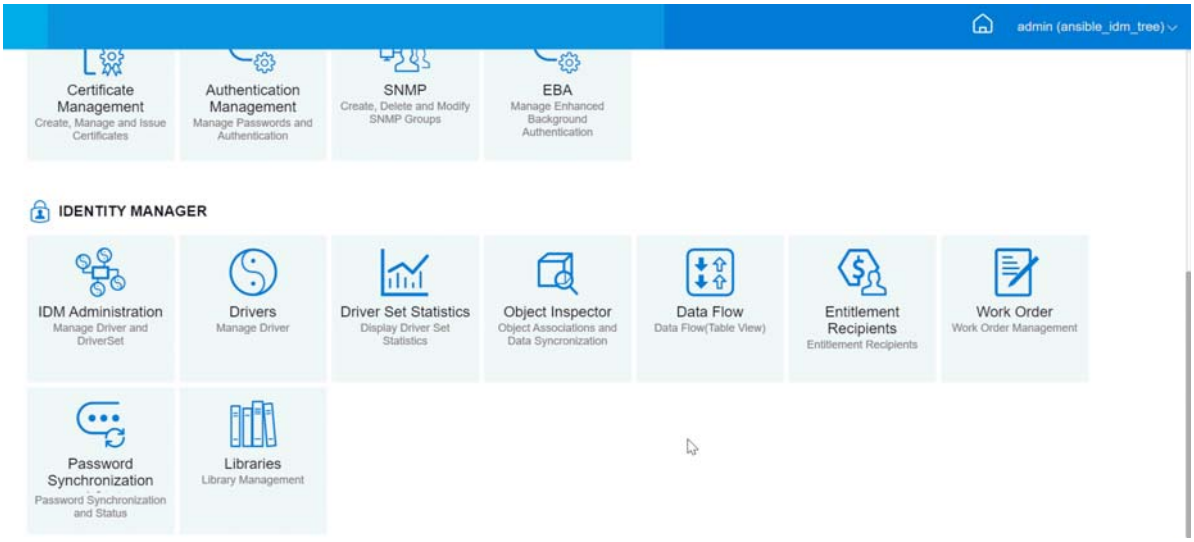
1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Arbeitsauftrag**.
2. Wählen Sie den zu löschenden Arbeitsauftrag aus.
3. Klicken Sie auf das Symbol .

Arbeitsauftragsliste filtern

Führen Sie die folgenden Schritte aus, um die Liste der Arbeitsaufträge zu filtern:

1. Klicken Sie auf der Identity Console-Landeseite auf die Option **Arbeitsauftrag**.
2. Klicken Sie unter „Arbeitsauftragsverwaltung“ auf **Aktionen**.
3. Wählen Sie im Dropdown-Menü den Filtertyp aus:
   - **Alle anzeigen:** Alle mit dem Treiber verknüpften Arbeitsaufträge werden aufgelistet.
   - **Konfiguriert:** Nur konfigurierte Arbeitsaufträge, die mit dem Treiber verknüpft sind, werden aufgelistet.
   - **Fehler:** Nur Arbeitsaufträge mit einem Fehlerstatus werden aufgelistet.
   - **Auf 'Warten' gelegt:** Arbeitsaufträge, die manuell in den Status „Wird gehalten“ versetzt wurden, werden aufgelistet.
   - **Ausstehend:** Arbeitsaufträge, die noch nicht fällig sind, werden aufgelistet.

Abbildung 28-1 *Arbeitsaufträge verwalten*



29 Passwortstatus und Passwortsynchronisierung verwalten

Sie können die Passwortsynchronisierung und den Passwortstatus einzelner Treiber im Identity Console-Portal überprüfen. Wählen Sie hierzu auf der Identity Console-Hauptseite das Modul **Passwortsynchronisierung** aus.

Mit diesem Modul können Sie die folgenden Aktionen ausführen:

- „Passwortsynchronisierungsstatus überprüfen“, auf Seite 199
- „Einstellungen für die Passwortsynchronisierung überprüfen“, auf Seite 200

Passwortsynchronisierungsstatus überprüfen

Sie können ermitteln, ob das Verteilungspasswort eines bestimmten Benutzers mit dem Passwort im verbundenen System identisch ist. Führen Sie die folgenden Schritte aus, um den Passwortsynchronisierungsstatus zu überprüfen:

1. Wählen Sie in Identity Console **Passwortsynchronisierung** > **Passwortstatus** aus.
2. Wählen Sie durch Durchsuchen einen Benutzer aus, für den Sie den Passwortstatus überprüfen möchten.
3. Die folgenden Passwortstatus können angezeigt werden:
   - Passwörter werden synchronisiert.
   - Passwörter werden NICHT synchronisiert.
   - Der Passwortstatus ist unbekannt, weil das verbundene System zur Prüfung des Passworts nicht kontaktiert werden kann.
   - Ein Fehler ist aufgetreten.

HINWEIS: Um weitere Details zu den oben genannten Status anzuzeigen, müssen Sie den Mauszeiger über den Status unter der Spalte **Passwortstatus** bewegen.

Die Aufgabe „Passwortstatus“ bewirkt, dass der Treiber die Aktion „Objektpasswort überprüfen“ ausführt. Nicht alle Treiber unterstützen die Passwortüberprüfung. Die Treiber, die dies unterstützen, müssen eine Passwortüberprüfungsfunktion im Treibermanifest enthalten. Identity Console lässt nicht zu, dass Passwortüberprüfungsvorgänge an Treiber gesendet werden, die diese Funktion nicht im Manifest enthalten.

Die Aktion „Objektpasswort überprüfen“ überprüft das Verteilungspasswort. Wenn das Verteilungspasswort nicht aktualisiert wird, meldet die Aktion „Objektpasswort überprüfen“ eventuell, dass die Passwörter nicht synchronisiert sind.

Das Verteilungspasswort wird in den folgenden Situationen nicht aktualisiert:

- Sie verwenden die Synchronisierungsmethode mit dem NDS-Passwort zum Synchronisieren oder dem universellen Passwort zum Synchronisieren. Weitere Informationen finden Sie im „Passwortrichtlinien mit benutzerdefinierten Einstellungen erstellen“, auf Seite 118.

HINWEIS: Die Aktion „Passwortstatus“ überprüft das NDS-Passwort anstelle des universellen Passworts für das Identitätsdepot. Wenn also in der Passwortrichtlinie des Benutzers keine Synchronisierung des NDS-Passworts mit dem universellen Passwort vorgesehen ist, wird immer gemeldet, dass die Passwörter nicht synchronisiert wurden. Das Verteilungspasswort und das Passwort auf dem verbundenen System können durchaus synchronisiert sein, die Aufgabe „Passwortstatus überprüfen“ liefert jedoch nur dann ein korrektes Ergebnis, wenn das NDS-Passwort und das Verteilungspasswort mit dem universellen Passwort synchronisiert wurden.

Einstellungen für die Passwortsynchronisierung überprüfen

Mit der Passwortsynchronisierung können Sie Passwörter in verbundenen Systemen mit Identity Manager synchronisieren. Um die Einstellungen für die Passwortsynchronisierung für verbundene Systeme anzuzeigen, wählen Sie den entsprechenden Treibersatz aus der Dropdown-Liste aus.

Mithilfe der Passwortsynchronisierung können folgende Funktionen für verbundene Systeme eingerichtet werden:

- Veröffentlichen von Passwörtern in Identity Manager
- Abonnieren von Passwörtern aus Identity Manager oder anderen verbundenen Systemen.
- Erzwingen von Passwortrichtlinien auf verbundenen Systemen
- Versenden von Benachrichtigungs-Emails

Führen Sie die folgenden Schritte aus, um die Einstellungen für die Passwortsynchronisierung zu überprüfen:

1. Wählen Sie auf der Identity Console-Hauptseite **Passwortsynchronisierung** > **Passwortsynchronisierung** aus.
2. Wählen Sie den Treibersatz aus, der den Treiber enthält, dessen Einstellungen Sie überprüfen möchten.
3. Klicken Sie in der Liste auf den Namen des Treibers.

   HINWEIS: Die aktivierten und deaktivierten Einstellungen variieren je nach Treiber. Es sind nur die Einstellungen für die vom Treiber unterstützten Funktionen verfügbar.

   ---

4. Stellen Sie sicher, dass die Einstellungen richtig konfiguriert sind.

   Identity Manager akzeptiert Passwörter (Herausgeberkanal): Wenn diese Option aktiviert ist, lässt Identity Manager zu, dass Passwörter vom verbundenen System zum Identitätsdepot weitergeleitet werden. Bei Deaktivierung dieser Option lässt das System nicht zu, dass `<password>`-Elemente an Identity Manager weitergeleitet werden. Sie werden von einer Passwortsynchronisierungsrichtlinie auf dem Herausgeberkanal aus XML entfernt.

Diese Einstellung gilt für Benutzerpasswörter, die vom verbundenen System selbst bereitgestellt werden, sowie für Passwortwerte, die von einer Richtlinie auf dem Herausgeberkanal erstellt werden.

Wenn diese Option aktiviert ist, aber die Option „Verteilungspasswort“ darunter deaktiviert ist, wird ein <password>-Wert vom verbundenen System direkt in das universelle Passwort im Identitätsdepot geschrieben. Falls die Passwortrichtlinie des Benutzers kein universelles Passwort zulässt, wird das Passwort zum NDS-Passwort geschrieben.

Verteilungspasswort für die Passwortsynchronisierung verwenden: Diese Einstellung ist nur verfügbar, wenn die Einstellung **Identity Manager akzeptiert Passwörter (Herausgeberkanal)** aktiviert ist.

Wenn diese Option aktiviert ist, werden Passwortwerte aus dem verbundenen System zum Verteilungspasswort geschrieben. Das Verteilungspasswort ist reversibel. Das heißt, es kann zur Passwortsynchronisierung aus der Identitätsdepot-Datenablage abgerufen werden. Es wird von Identity Manager für die bidirektionale Passwortsynchronisierung mit verbundenen Systemen verwendet. Damit Identity Manager Passwörter von diesem System an andere Systeme verteilen kann, muss diese Option aktiviert sein.

Passwort nur akzeptieren, wenn es die Passwortrichtlinie des Benutzers erfüllt: Diese Einstellung ist nur verfügbar, wenn die Einstellung **Verteilungspasswort für Passwortsynchronisierung verwenden** aktiviert ist.

Wenn die Option aktiviert ist, schreibt Identity Manager das Passwort von diesem verbundenen System nur dann zum Verteilungspasswort im Identitätsdepot und veröffentlicht es nur dann an andere verbundene Systeme, wenn das Passwort die Passwortrichtlinie des Benutzers erfüllt.

Wenn ein Passwort die Richtlinie nicht erfüllt, aktivieren Sie die Einstellung **Reset the user's password to the Distribution Password** (Benutzerpasswort auf Verteilungspasswort zurücksetzen), um das Benutzerpasswort auf dem verbundenen System zurückzusetzen. Auf diese Weise können Sie die Passwortrichtlinie sowohl auf dem verbundenen System als auch im Identitätsdepot erzwingen. Wenn Sie diese Option nicht aktivieren, kann es zu asynchronen Benutzerpasswörtern auf verbundenen Systemen kommen. Sie müssen jedoch die Passwortrichtlinien des verbundenen Systems berücksichtigen, wenn Sie erwägen, diese Option zu verwenden. Einige verbundene Systeme lassen das Zurücksetzen möglicherweise nicht zu, da sie die wiederholte Nutzung von Passwörtern nicht gestatten.

Mithilfe der Einstellung **Benutzer per Email über Fehler bei der Passwortsynchronisierung benachrichtigen** können Sie Benutzer informieren, wenn ein Passwort nicht festgelegt oder zurückgesetzt werden kann. Die Benachrichtigungsoption ist für diese Option besonders hilfreich. Wenn der Benutzer ein Passwort ändert, das für das verbundene System zulässig ist, aber aufgrund der Passwortrichtlinie von Identity Manager zurückgewiesen wird, erfährt der Benutzer erst, dass das Passwort zurückgesetzt wurde, wenn er eine entsprechende Benachrichtigung erhält oder wenn er versucht, sich mit dem alten Passwort anzumelden.

Passwort immer akzeptieren, Passwortrichtlinien ignorieren: Diese Einstellung ist nur verfügbar, wenn die Einstellung **Verteilungspasswort für Passwortsynchronisierung verwenden** aktiviert ist.

Wenn Sie diese Option auswählen, erzwingt Identity Manager die Umsetzung der Passwortrichtlinie des Benutzers für das verbundene System nicht. Identity Manager schreibt das Passwort von diesem verbundenen System in das Verteilungspasswort im Identitätsdepot und verteilt es unabhängig von der Erfüllung der Passwortrichtlinie an andere verbundene Systeme.

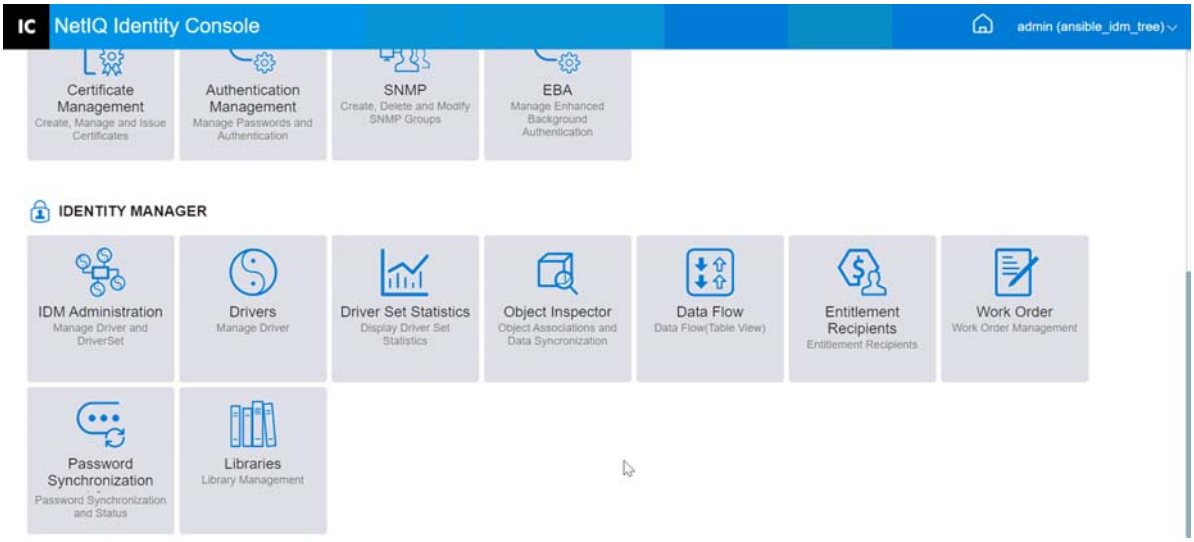
Anwendung akzeptiert Passwörter (Abonnentenkanal): Wenn Sie diese Option aktivieren, sendet der Treiber Passwörter aus dem Identitätsdepot an dieses verbundene System. Wenn ein Benutzer dann sein Passwort auf einem anderen verbundenen System ändert, das Passwörter als Verteilungspasswort im Identitätsdepot veröffentlicht, wird das Passwort für dieses verbundene System ebenfalls geändert.

Standardmäßig ist das Verteilungspasswort mit dem universellen Passwort im Identitätsdepot identisch, sodass Änderungen am universellen Passwort im Identitätsdepot auch an das verbundene System weitergegeben werden.

Benutzer bei Passwortsynchronisierungsfehler per Email benachrichtigen: Wenn Sie diese Option aktivieren, erhält der Benutzer eine Email, wenn ein Passwort nicht synchronisiert, festgelegt oder zurückgesetzt werden konnte. Diese Email basiert auf einer Email-Schablone. Diese Schablone wird von der Passwortsynchronisierungsanwendung bereitgestellt. Damit sie funktioniert, müssen Sie sie jedoch anpassen und einen Email-Server angeben, der die Benachrichtigungen versenden soll. Anweisungen finden Sie unter Configuring E-Mail Notification (Konfigurieren von Email-Benachrichtigungen) im *NetIQ Identity Manager Password Management Guide* (NetIQ Identity Manager-Passwortverwaltungshandbuch).

5 Wenn Sie fertig sind, klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern. Die Einstellungen werden als globale Konfigurationswerte gespeichert.

Abbildung 29-1 *Passwortsynchronisierung verwalten*



30 Bibliotheken verwalten

Bibliotheksobjekte speichern mehrere Richtlinien und andere Ressourcen, die von einem oder mehreren Treibern gemeinsam genutzt werden. Ein Bibliotheksobjekt kann in einem Treibersatzobjekt oder einem beliebigen eDirectory-Container erstellt werden. In einem eDirectory-Baum können mehrere Bibliotheken vorhanden sein. Treiber können auf jede Bibliothek im Baum verweisen, solange der Server, auf dem der Treiber ausgeführt wird, ein Lese-/Schreib- oder Masterreplikat des Bibliotheksobjekts enthält.

Formatvorlagen, Richtlinien, Regeln und andere Ressourcenobjekte können in einer Bibliothek gespeichert und von einem oder mehreren Treibern referenziert werden.

Mit dem Bibliotheksverwaltungsmodul können Sie die folgenden Aufgaben ausführen:

- „Vorhandene Bibliotheken anzeigen und löschen“, auf Seite 203
- „Objekte der Bibliothek anzeigen oder löschen“, auf Seite 203

Vorhandene Bibliotheken anzeigen und löschen

Führen Sie die folgenden Schritte aus, um eine vorhandene Bibliothek anzuzeigen oder zu löschen:

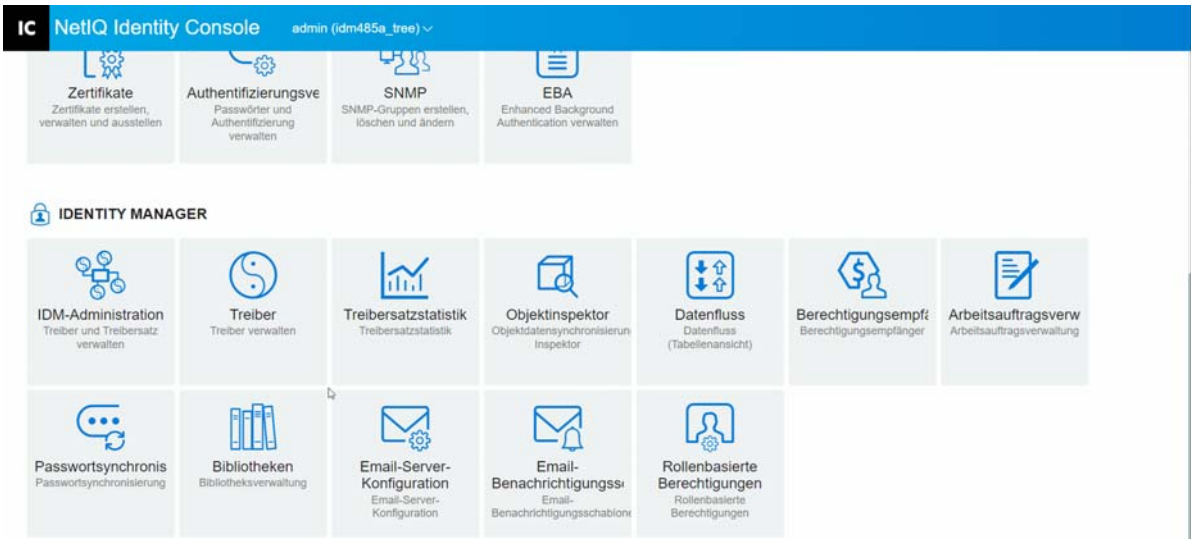
1. Wählen Sie in Identity Console auf der Startseite das Modul **Bibliotheken** aus.
2. Wählen Sie die entsprechende Bibliothek aus der Liste aus.
3. Klicken Sie auf das Symbol  . Klicken Sie zur Bestätigung auf **OK**.

Objekte der Bibliothek anzeigen oder löschen

Sie können Richtlinien und Zuordnungstabellen aus Bibliotheksobjekten anzeigen und löschen. Führen Sie die folgenden Schritte aus, um Objekte zu löschen:

1. Wählen Sie in Identity Console auf der Startseite das Modul **Bibliotheken** aus.
2. Klicken Sie in der Liste auf die entsprechende Bibliothek.
3. Um Richtlinien zu löschen, wählen Sie die Registerkarte **Richtlinien** aus.
4. Wählen Sie die entsprechende Richtlinie aus der Liste aus und klicken Sie auf das Symbol  .
5. Um Zuordnungstabellen zu löschen, wählen Sie die Registerkarte **Zuordnungstabellen** aus.
6. Wählen Sie die entsprechende Zuordnungstabelle aus der Liste aus und klicken Sie auf das Symbol  .
7. Klicken Sie zur Bestätigung auf **OK**.

Abbildung 30-1 *Bibliotheken verwalten*



31 Email-Serveroptionen verwalten

Über die Email-Serveroptionen können Sie die Einstellungen für Ihren SMTP-Email-Server festlegen.

Hostname

Der Hostname des SMTP-Email-Servers. Hierbei kann es sich auch um eine IP-Adresse handeln. Sie können auch einen benutzerdefinierten Port gefolgt vom Hostnamen oder der IP-Adresse angeben.

WICHTIG: Verwenden Sie zwischen dem Hostnamen oder der IP-Adresse und dem Port einen Doppelpunkt (:) als Trennzeichen.

Von

Sie können eine gültige Email-Adresse angeben, die als Von-Feld im Email-Header angezeigt wird.

Zeitüberschreitungswert

Mit der Zeitüberschreitungsoption können Sie einen Zeitüberschreitungswert (in Sekunden) für das Senden von Benachrichtigungs-Emails festlegen.

SSL aktivieren

Je nach Bedarf können Sie die SSL-Option aktivieren.

Mit Berechtigungsnachweis bei Server authentifizieren

Verwenden Sie diese Option für einen gesicherten SMTP-Server. Muss der Server vor dem Senden von Email authentifiziert werden, geben Sie den Benutzernamen und das Passwort an dieser Stelle an.

Obwohl die Authentifizierungsinformationen an dieser Stelle festgelegt werden, müssen sie für die Anwendung, die die Benachrichtigungs-Emails sendet, unter Umständen nochmals angegeben werden.

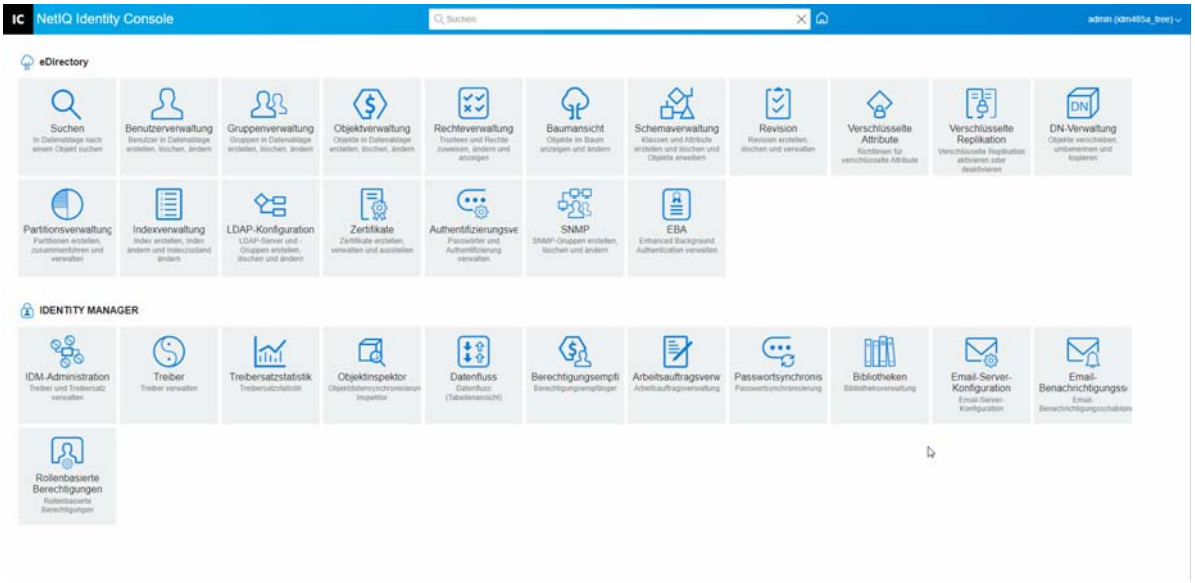
Sie können die hier angegebenen Authentifizierungsinformationen beispielsweise verwenden, um Email-Benachrichtigungen bei vergessenen Passwörtern zu versenden. Die Identity Manager-Passwortsynchronisierung setzt jedoch die Treiberrichtlinie ein, um Benachrichtigungs-Emails zu versenden. Möglicherweise müssen Sie die Authentifizierungsinformationen auch in dieser Treiberrichtlinie angeben.

Führen Sie die folgenden Schritte aus, um den Server zu authentifizieren:

1. Wählen Sie die Option **Mit Berechtigungsnachweis am Server authentifizieren** aus.
2. Geben Sie unter **Benutzername** und **Passwort** die entsprechenden Angaben ein.
3. Klicken Sie auf **Serververbindung testen**, um die Konnektivität zu überprüfen.
4. Klicken Sie auf **Speichern**.

HINWEIS: Nachdem Sie den Berechtigungsnachweis gespeichert haben, wird die Option **Serververbindung testen** deaktiviert.

Abbildung 31-1 *Email-Server-Konfiguration*



32 Email-Schablonen verwalten

Diese Liste enthält die verfügbaren Benachrichtigungsschablonen. Mit diesen Schablonen können Sie Email-Nachrichten an Benutzer dieses Baums versenden. Sie können diese Schablonen mit benutzerdefiniertem Text anpassen.

Einige Anwendungen haben ihre eigenen Schablonen. Diese Schablonenobjekte sind im Sicherheitscontainer gespeichert, der sich in der Regel im Stammverzeichnis des Baums befindet.

Sie können die Liste nach Name, Datum oder Betreff sortieren.

Betreff

Hier wird der Text eingegeben, den der Benutzer in der Betreffzeile einer Email sehen kann. Um die Schablone zu bearbeiten, klicken Sie auf die Betreffzeile der Schablone. Über die Option „Email-Benachrichtigungsschablonen bearbeiten“ können Sie die Schablone und ihre Details ändern.

Schablonenname

Jede Schablone hat einen eindeutigen Namen. Dieser Name wird von der Anwendung verwendet, die die Email versendet.

Zuletzt geändert

Das Datum und die Uhrzeit der letzten Änderung der Schablone.

Neu

Diese Option ermöglicht das Erstellen einer neuen Email-Schablone.

1. Klicken Sie auf das Symbol +.
2. Geben Sie einen Namen für die neue Schablone ein (z. B. Genehmigung) und klicken Sie auf **OK**.

Wenn Sie Popups deaktiviert haben, kehren Sie zum Popup „Email-Benachrichtigungsschablonen bearbeiten“ zurück. Die neue Schablone wird in der Spalte "Name" aufgeführt, wobei der Eintrag in der Spalte für die Betreffzeile "[Kein Betreff]" lautet. In diesem Fall sollten Sie auf [Kein Betreff] klicken, um die Details der neuen Schablone eingeben zu können.

Email-Benachrichtigungsschablonen bearbeiten

Auf der Seite „Email-Benachrichtigungsschablonen bearbeiten“ können Sie die Email-Schablone ändern. Sie können die Schablonen mit benutzerdefiniertem Text anpassen.

Schablonenname

Zeigt den Namen der Schablone an.

Betreff

Hier wird der Text eingegeben, den der Benutzer in der Betreffzeile einer Email sehen kann. Sie können den Text der Betreffzeile anpassen. Der eigentliche Name der Schablone wird dadurch nicht geändert.

Senden als

Das Format, das der SMTP-Server zum Senden der Email verwendet: Text oder HTML.

Token oder Platzhalter-Tags

Mithilfe von Platzhalter-Tags kann die Nachricht für den Benutzer personalisiert werden. Sie können Platzhalter-Tags aus der Liste der verfügbaren Tags kopieren und in die Nachricht einfügen.

Jede Schablone enthält standardmäßige Token oder Platzhalter-Tags. Hierbei handelt es sich um Variablen, die zum Personalisieren der Email für den Benutzer benötigt werden. Die Email-Schablone „Passwort vergessen“ zum Senden eines Passworts an den Benutzer umfasst beispielsweise das standardmäßige Token bzw. Platzhalter-Tag „$CurrentPassword“.

Hinzufügen: Sie können andere Token oder Platzhalter-Tags zur Verwendung im Nachrichtentext festlegen.

Führen Sie die die folgenden Schritte aus, um Token oder Platzhalter-Tags hinzuzufügen:

1. Klicken Sie auf das Symbol  .
2. Geben Sie unter **Name** und **Beschreibung** im Fenster **Platzhalter-Tag hinzufügen** die entsprechenden Angaben ein.
3. Klicken Sie auf **OK**.
4. Das neue Token oder Platzhalter-Tag wird in der Spalte „Platzhalter-Tags“ aufgeführt.

Tag kopieren: Klicken Sie auf  , um das ausgewählte Tag in den Systempuffer zu kopieren, und klicken Sie dann mit der Maustaste, um es einzufügen und in der Betreffzeile oder im Textkörper der Nachricht zu verwenden.

Löschen: Wähle ein Token oder ein Platzhalter-Tag in der Liste aus und klicken Sie auf  , um das Tag aus der Liste zu löschen. Achten Sie darauf, keine Tags zu entfernen, die für den Nachrichtentext benötigt werden.

Nachrichtentext

Der Text der Email-Nachricht.

Klicken Sie auf **Aktualisieren**, nachdem Sie alle Änderungen an der Email-Benachrichtigungsschablone angegeben haben.

Löschen

Mit dieser Option werden von Ihnen erstellte Schablonen (aus dem Identitätsdepot) gelöscht. Standardschablonen, die im Lieferumfang von Anwendungen wie Identity Manager enthalten sind, können nicht gelöscht werden.

1. Wähle die zu löschende Schablone aus.

Wenn Sie auf die Betreffzeile der Schablone klicken, ruft Identity Console das Dialogfeld „Email-Schablonen bearbeiten“ auf.

2. Klicken Sie auf das Löschsymbol.
3. Klicken Sie auf **OK**.

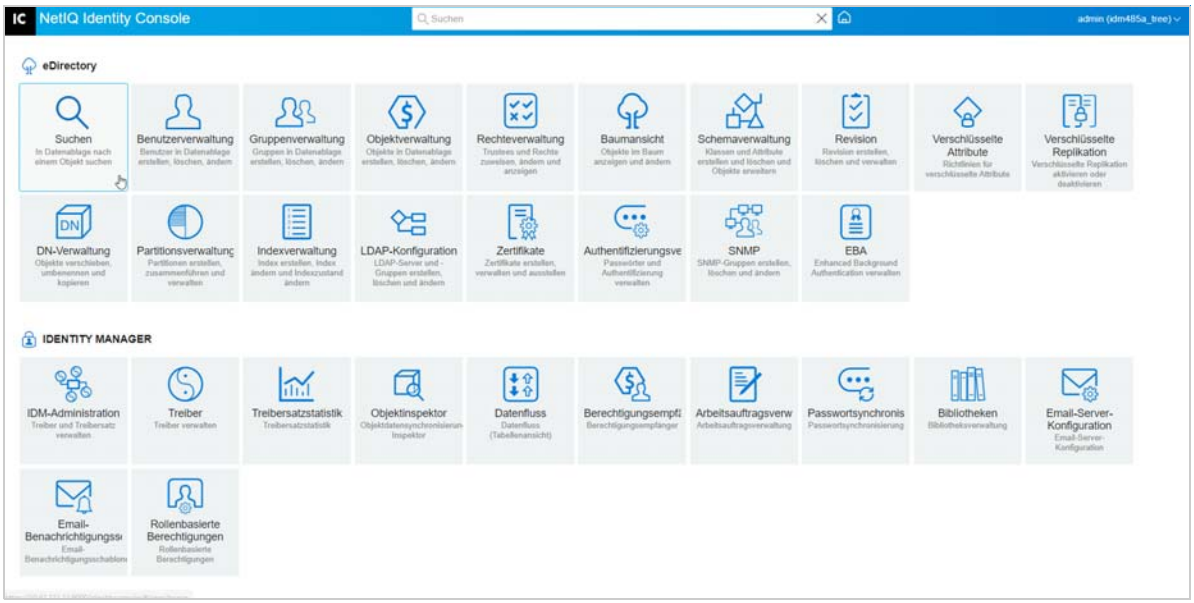
Schablonen filtern

Mit dieser Option können Sie filtern, welche Email-Schablonen angezeigt werden sollen. Nur die ausgewählten Schablonen werden angezeigt. Mit der Option „Filtern nach – Alle anzeigen“ werden alle Schablonen angezeigt.

Schablonen aktualisieren

Klicken Sie auf das Symbol , um die Anzeige zu aktualisieren und alle angewendeten Filterschablonen zu entfernen.

Abbildung 32-1 *Email-Benachrichtigungsschablonen*



33 Rollenbasierte Berechtigungen verwalten

Mit RBE können Sie einer Gruppe von NetIQ® Identity Console-Benutzern Berechtigungen für verbundene Systemen gewähren. Mithilfe von RBE-Richtlinien lässt sich die Verwaltung von Geschäftsrichtlinien vereinfachen und der Konfigurationsaufwand für die Identity Manager-Treiber wird reduziert.

Das Modul „Rollenbasierte Berechtigung“ umfasst Folgendes:

Rollenbasierte Berechtigung

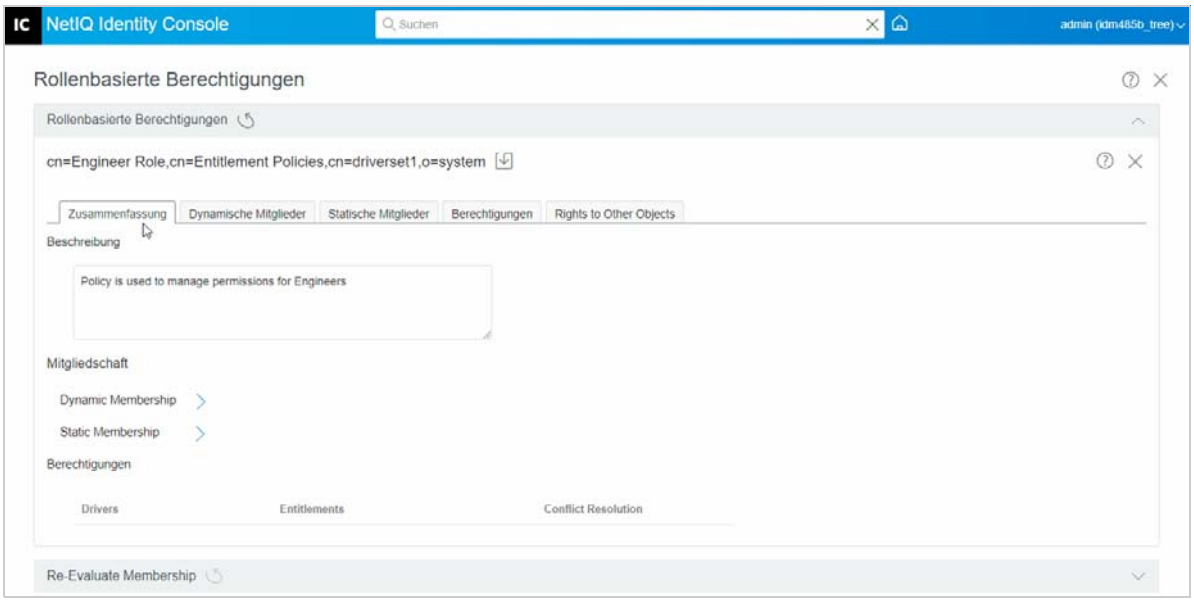
Eine RBE-Richtlinie ist ein dynamisches Identity Console-Gruppenobjekt mit zusätzlichen Funktionen zum Erteilen von RBE für verbundene Systeme. Beim Erstellen einer RBE-Richtlinie definieren Sie die Mitgliedschaft für die Richtlinie und die Berechtigungen, die den Mitgliedern der RBE-Richtlinie erteilt werden sollen. Jede RBE-Richtlinie wird einem einzelnen Treibersatzobjekt zugeordnet, das einem bestimmten Server zugewiesen wird. Wie ein Identity Manager-Treiber kann eine Berechtigungsrichtlinie nur Objekte verwalten, die sich in einer Master- oder einer Lese-/Schreibreproduktion auf dem Server befinden, dem sie zugewiesen ist.

In den folgenden Abschnitten wird die rollenbasierte Berechtigung ausführlich erläutert:

Zusammenfassung

Diese Seite enthält eine allgemeine Übersicht über die Mitgliedschaftskriterien und die Berechtigungen für eine Berechtigungsrichtlinie.

Abbildung 33-1 *Seite „Zusammenfassung“*



Mitgliedschaft:

Die für die dynamische Mitgliedschaft angegebenen Kriterien werden in der Syntax eines LDAP-Filters angezeigt. Unter "Suchidentität" steht, wessen Objektrechte bei Abfragen für die dynamische Mitgliedschaft verwendet werden. "Basis-DN" und "Bereich" geben an, welche Teile des Baums in die Abfrage einbezogen werden.

Welche Mitglieder durch statische Mitgliedschaften einbezogen oder ausgeschlossen wurden, kann durch Auswahl des entsprechenden Kontrollkästchens angegeben werden.

Die kombinierte Liste aller Mitglieder wird nicht auf der Zusammenfassungsseite angezeigt, da die Liste sehr lang sein kann. Eine solche kombinierte Liste aller Mitglieder der Berechtigungsrichtlinie (dynamisch und statisch) finden Sie unter "Mitgliedschaft > Mitgliedschaft anzeigen".

Berechtigungen:

Hier werden die Berechtigungen für verbundene Systeme angezeigt, die Mitgliedern der Berechtigungsrichtlinie erteilt wurden. Beachten Sie, dass funktionsbasierte Berechtigungen nur grob mit dem verbundenen System übereinstimmen. Das bedeutet, dass der Status einer Berechtigung in einem verbundenen System in der Benutzeroberfläche für Berechtigungsrichtlinien nicht angezeigt wird. Wenn Sie einer Berechtigungsrichtlinie eine Berechtigung zuweisen und diese Berechtigung später auf dem verbundenen System nicht mehr verfügbar ist, bleibt sie dennoch solange in der Berechtigungsrichtlinie aufgeführt, bis sie manuell aus der Liste entfernt wird.

Konfliktlösung:

Bei RBE mit Werten wird mit der hier angegebenen Methode festgelegt, welche Werte einem Benutzer erteilt werden, wenn mindestens zwei RBE-Richtlinien diesem Benutzer unterschiedliche Werte zuweisen. Eine Berechtigung mit Werten ist beispielsweise die Mitgliedschaft in Email-Verteilerlisten, bei denen die Werte die Namen der Verteilerlisten darstellen.

Die Konfliktlösungsmethode wird separat für jede einzelne Berechtigung jedes Treiberobjekts festgelegt. Wenn eine Berechtigung in mehreren RBE-Richtlinien eingesetzt wird, gilt die entsprechende Konfliktlösungsmethode für alle diese RBE-Richtlinien. Um eine andere Konfliktlösungsmethode für eine Berechtigung zu wählen, ändern Sie die Einstellung für diese Berechtigung im Treibermanifest des entsprechenden Treibers.

- **Nicht erkannt:** Die RBE-Richtlinie wurde im Assistenten nicht abgeschlossen oder die Einstellung wurde fehlerhaft im Treibermanifest eingegeben.
- **Zusammenführen:** Die Standardeinstellung ist „Zusammenführen“ (`union` im Treibermanifest). Bei dieser Einstellung werden einem Benutzer alle Werte für die Berechtigung aus allen RBE-Richtlinien erteilt, deren Mitglied er ist.

  Mit der Standardeinstellung „Zusammenführen“ spielt die Priorität, d. h. die Reihenfolge in der Liste der Richtlinien, für die jeweilige Berechtigung keine Rolle.

  Angenommen, einem Benutzer werden auf Grundlage zweier unterschiedlicher RBE-Richtlinien (Administratorrichtlinie und Team-Mitglieder-Richtlinie) Mitgliedschaften in Email-Verteilerlisten für den GroupWise®-Treiber A erteilt. In der ersten Richtlinie wird dem Benutzer die Mitgliedschaft in der Email-Verteilerliste für Administratoren erteilt und in der zweiten Richtlinie erhält er die Mitgliedschaft in der Email-Verteilerliste für Team-Mitglieder. Wenn die Einstellung "Zusammenführen" lautet, wird dem Benutzer die Mitgliedschaft in beiden Email-Verteilerlisten erteilt.
- **Priorität:** Wenn mehrere RBE-Richtlinien für ein Treiberobjekt einem Benutzer unterschiedliche Werte für dieselbe Berechtigung zuweisen, werden dem Benutzer bei dieser Einstellung nur die Werte aus der RBE-Richtlinie erteilt, die in der Liste am weitesten oben steht.

  Bei der Einstellung „Priorität“ spielt die Priorität, d. h. die Reihenfolge in der Liste der Richtlinien, für die jeweilige Berechtigung eine wichtige Rolle.

  Angenommen, einem Benutzer werden auf Grundlage zweier unterschiedlicher RBE-Richtlinien (Administratorrichtlinie und Team-Mitglieder-Richtlinie) Mitgliedschaften in Email-Verteilerlisten für den GroupWise-Treiber A erteilt. In der Administratorrichtlinie wird dem Benutzer die Mitgliedschaft in der Email-Verteilerliste für Administratoren erteilt und in der Team-Mitglieder-Richtlinie erhält er die Mitgliedschaft in der Email-Verteilerliste für Team-Mitglieder. Die Administratorrichtlinie steht in der Liste der Richtlinien weiter oben als die Team-Mitglieder-Richtlinie. Wenn die Einstellung "Priorität" lautet, wird dem Benutzer nur die Mitgliedschaft in der Email-Verteilerliste für Administratoren erteilt.

  Diese Konfliktlösungseinstellung eignet sich beispielsweise dann, wenn ein Attribut für das verbundene System nur einen einzelnen Wert zulässt. Wenn zwei unterschiedliche RBE-Richtlinien einem Benutzer jeweils einen Wert für dieses Attribut zuweisen, wird dem Benutzer die Berechtigung aus der RBE-Richtlinie erteilt, die in der Liste am weitesten oben steht.

HINWEIS: Für Berechtigungen ohne Werte, z. B. ein Konto, gibt es keine Konfliktlösungseinstellung. Berechtigungen ohne Werte werden den Mitgliedern einer RBE-Richtlinie unabhängig von der Priorität der Richtlinien in der Liste immer erteilt.

Dynamische Mitglieder

Die für die dynamische Mitgliedschaft angegebenen Kriterien werden in der Syntax eines LDAP-Filters angezeigt. Unter "Suchidentität" steht, wessen Objektrechte bei Abfragen für die dynamische Mitgliedschaft verwendet werden. "Basis-DN" und "Bereich" geben an, welche Teile des Baums in die Abfrage einbezogen werden.

Mitgliedschaftsfilter

Mit dieser Methode können Sie Mitgliedschaftskriterien wie die Position im Baum und die Attribute des Objekts definieren. Die Mitgliedschaft kann beispielsweise davon abhängen, ob sich der Benutzer im Aktivcontainer befindet oder ob seine Stellenbezeichnung das Wort „Manager“ enthält. Benutzer, die die Kriterien erfüllen, werden automatisch Mitglieder der RBE-Richtlinie, ohne dass sie einzeln zur Richtlinie hinzugefügt werden müssen. Die dynamische Mitgliedschaft entspricht einem dynamischen Gruppenobjekt.

Wenn sich ein Objekt ändert und die Kriterien für die dynamische Mitgliedschaft nicht mehr erfüllt, werden die Berechtigungen bei der nächsten Bewertung des Benutzers automatisch entzogen.

Suchparameter festlegen

Mit dieser Option können Sie die Position der Benutzer festlegen, die von der Berechtigungsrichtlinie verwaltet werden sollen. Wählen Sie den Container mit den Benutzern (Basis-DN) aus und geben Sie an, wie weit unterhalb dieses Containers sich die Suche erstrecken soll (Suchbereich). Damit die Benutzer in dem angegebenen Container von der Berechtigungsrichtlinie verwaltet werden können, müssen sich die Benutzer in einer Lese-/Schreib- oder einer Masterreproduktion des Servers befinden.

Die folgenden Optionen können für den Suchbereich ausgewählt werden:

- Dieser Container und Untercontainer: Benutzer, die diesem Container im Baum untergeordnet sind, gehören der Berechtigungsrichtlinie an, wenn sie die Kriterien für die dynamische Mitgliedschaft erfüllen. Benutzer in den Untercontainern sind ebenfalls Mitglieder, sofern sie die Kriterien erfüllen.
- Nur dieser Container: Benutzer aus diesem Container gehören nur dann der Berechtigungsrichtlinie an, wenn sie die für die dynamische Mitgliedschaft angegebenen Kriterien erfüllen. Benutzer aus Untercontainern dieses Containers sind keine Mitglieder, auch wenn sie die Kriterien erfüllen.

Filterkriterien definieren

Mit dieser Option können Sie die Merkmale festlegen, mit denen bestimmt wird, welche Benutzer Mitglied der Berechtigungsrichtlinie werden.

Auf der Zusammenfassungsseite einer Berechtigungsrichtlinie werden die von Ihnen angegebenen Kriterien für die dynamische Mitgliedschaft in der Syntax eines LDAP-Filters angezeigt.

Standardmäßig ist die dynamische Mitgliedschaft so eingerichtet, dass alle Benutzerklassenobjekte (und Objekte aus Klassen, die sich aus der Benutzerklasse ableiten) innerhalb des Suchbereichs Mitglieder der Berechtigungsrichtlinie sind.

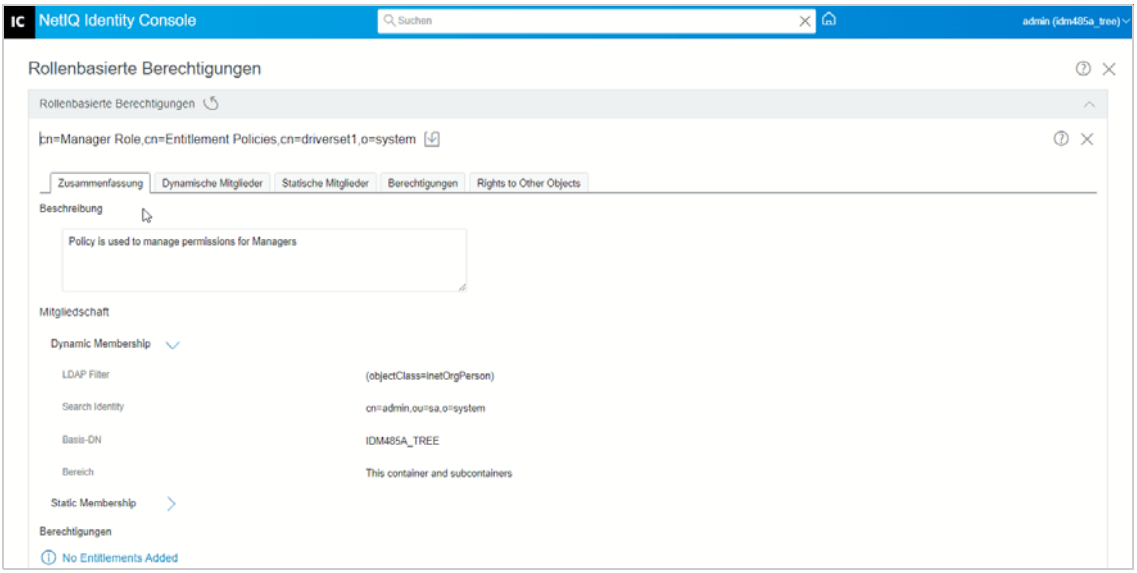
HINWEIS: Wenn Sie eine neue Objektklasse erstellen, die von einem Benutzer abgeleitet ist, wird diese erst dann in eine vorhandene Berechtigungsrichtlinie aufgenommen, wenn Sie Änderungen an der Berechtigungsrichtlinie vornehmen. So wird verhindert, dass Benutzern der neuen Klassen unabsichtlich Berechtigungen erteilt werden. Beim Ändern der Berechtigungsrichtlinie wird die Liste der aus der Benutzerklasse abgeleiteten Klassen für diese Richtlinie aktualisiert.

Dynamische Mitgliedschaft erstellen

Führen Sie auf der Registerkarte „Dynamische Mitglieder“ die folgenden Schritte aus:

1. Klicken Sie auf die Registerkarte **Dynamische Mitglieder**.
2. Verwenden Sie je nach Bedarf die Filter **Suchidentität**, **Suche beginnen bei** und **Suchbereich**.
3. Klicken Sie auf die spezifische Option **Gruppe erstellen**, um eine neue Bedingung oder Zeile zu erstellen, und geben Sie dann die erforderlichen Suchkriterien oder Bedingungen an.

Abbildung 33-2 *Dynamische Mitglieder*



Suchbereich: Der Suchbereich legt den Satz an Einträgen auf oder unter dem Niveau des Suchbasis-DN fest, die als mögliche Treffer für den Suchvorgang berücksichtigt werden sollen.

Suchkriterien: Sie können eine Suche einschränken, um einen bestimmten Datensatz oder eine Gruppe von Datensätzen aus einer großen Anzahl von Datensätzen zu finden.

Basis-DN: Ein Basis-DN ist der Punkt, von dem aus ein Server nach Benutzern sucht.

LDAP-Gruppe: Sie stellt eine hierarchische Organisation von Benutzern, Gruppen und Organisationseinheiten dar, die Container für Benutzer und Gruppen sind.

HINWEIS: Der Benutzer kann einzelne oder mehrere Gruppen mit Bedingungen erstellen. Die Bedingungen bestehen aus Attributen, Operatoren und Werten. Standardmäßig ist **Objektklasse** > **ist gleich** > **Benutzer** ausgefüllt.

Statische Mitglieder

Statische Mitglieder sind Mitgliederklassen, die mit statischen Schlüsselwörtern deklariert werden. Ein statisches Mitglied hat bestimmte eingeschränkte Zugriffe.

Auf der Registerkarte „Statische Mitglieder“ können Sie die folgenden Aktionen ausführen:

Mitglieder einschließen:

Sie können Mitglieder, die nicht im Filter für die dynamische Mitgliedschaft enthalten sind, statisch hinzufügen.

Mitglieder ausschließen:

Sie können Mitglieder ausschließen, die zwar die Kriterien des Filters erfüllen, aber nicht in die Berechtigungsrichtlinie einbezogen werden sollen.

Berechtigungen

Mit RBE können Sie Berechtigungen auf verbundenen Systemen und Rechte in Identity Manager gewähren. Folgende Berechtigungen können vergeben werden:

- Konten auf verbundenen Systemen.
- Mitgliedschaft in Email-Verteilerlisten für verbundene Systeme.
- Gruppenmitgliedschaft für verbundene Systeme.
- Attribute für die entsprechenden Objekte in verbundenen Systemen, die mit den von Ihnen angegebenen Werten belegt sind.

HINWEIS: Da die Funktionen für rollenbasierte Berechtigungen Teil von Identity Manager sind, müssen Identity Manager-Treiber installiert und für rollenbasierte Berechtigungen konfiguriert sein, damit Sie Berechtigungen für verbundene Systeme erteilen können.

Berechtigung erstellen

Führen Sie auf der Registerkarte „Berechtigungen“ die folgenden Schritte aus:

1. Klicken Sie auf die Registerkarte **Berechtigung**.
2. Klicken Sie auf +, um **Treiber hinzufügen** zu können und Berechtigungen für verbundene Systeme bereitzustellen.

   Der Bildschirm **Treiber hinzufügen** wird angezeigt.
3. Wählen Sie den Treiber im Dropdown-Menü aus.
4. Klicken Sie auf **Hinzufügen**.

   Der Bildschirm **Berechtigungen hinzufügen** wird angezeigt.
5. Wählen Sie im Dropdown-Menü **Berechtigung auswählen** die Gruppe aus, die Sie hinzufügen möchten.
6. Wählen Sie den **Abfragetyp** aus:
   - **Im Cache gespeichert:** Für zuvor ausgeführte Abfragen.
   - **Externe Abfrage:** Für neue Abfragen.

   Der Bildschirm **Gruppenberechtigung hinzufügen** wird angezeigt.
7. Wählen Sie „Gruppenberechtigung“ im Dropdown-Menü aus und klicken Sie dann auf **Auswählen**.

Rechte für andere Objekte

Auf dieser Seite können Sie eDirectory-Objekten Trustee-Rechte für Berechtigungsrichtlinien zuweisen. Jedes Mitglied der Berechtigungsrichtlinie wird zum Trustee des Objekts.

Zusätzlich zum Zuweisen von Rechten für alle Attribute können Sie auf „Eigenschaft hinzufügen“ klicken, um Rechte für bestimmte Eigenschaften zuzuweisen.

Mit dem Kontrollkästchen zum Übernehmen von Rechten kann festgelegt werden, ob die Rechte an untergeordnete Objekte im Baum weitergegeben werden. Wenn Sie beispielsweise Rechte für ein Containerobjekt zuweisen und möchten, dass die Berechtigungsrichtlinie dieselben Rechte auch den Objekten und Untercontainern des Containers zuweist, aktivieren Sie das Kontrollkästchen „Vererben“.

Rechte für Objekte werden den Mitgliedern der Berechtigungsrichtlinie in eDirectory erteilt, nachdem Sie die Änderungen auf dieser Seite abgeschlossen haben. Berechtigungen für verbundene Systeme werden im Gegensatz dazu allen Mitgliedern der Berechtigungsrichtlinie erteilt, wenn das nächste Mal ein Attribut für die dynamische Mitgliedschaft des Benutzers geändert oder der Benutzer verschoben bzw. umbenannt wird. (Dasselbe gilt auch für das Entziehen von Rechten und Berechtigungen.) Mit der Option "Mitgliedschaft neu bewerten" können Aktualisierungen erzwungen werden.

Rechte für andere Objekte erstellen

So erstellen Sie Rechte:

1 Klicken Sie auf die Registerkarte **Rechte für andere Objekte**

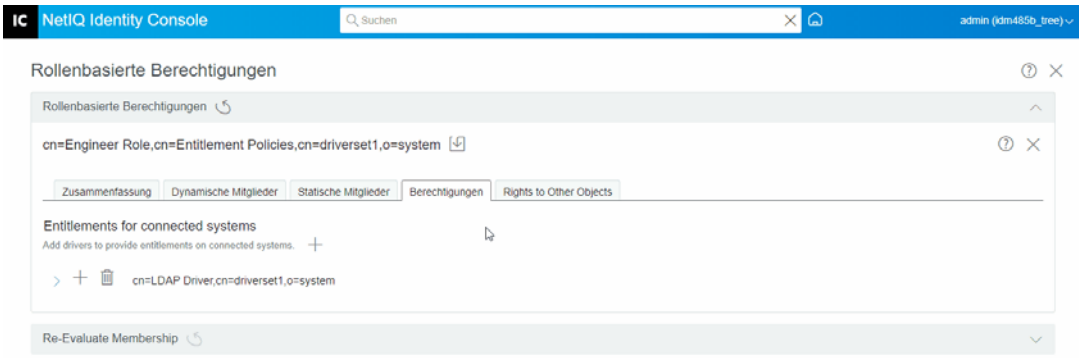
Hier können Sie ein neues Objekt hinzufügen und nach den Objekten suchen, für die diese Berechtigungsrichtlinie als Trustee festgelegt werden soll.

1a Um ein Objekt hinzuzufügen, klicken Sie auf die Schaltfläche  .

Die **KONTEXTBROWSER**-Seite wird angezeigt. Die Seite enthält `Objekte`.

1b Erweitern Sie die `Objekte`, wählen Sie je nach Bedarf Gruppen oder einzelne Benutzer aus und weisen Sie diesen Rechte zu.

Abbildung 33-3 *Rechte für andere Objekte*

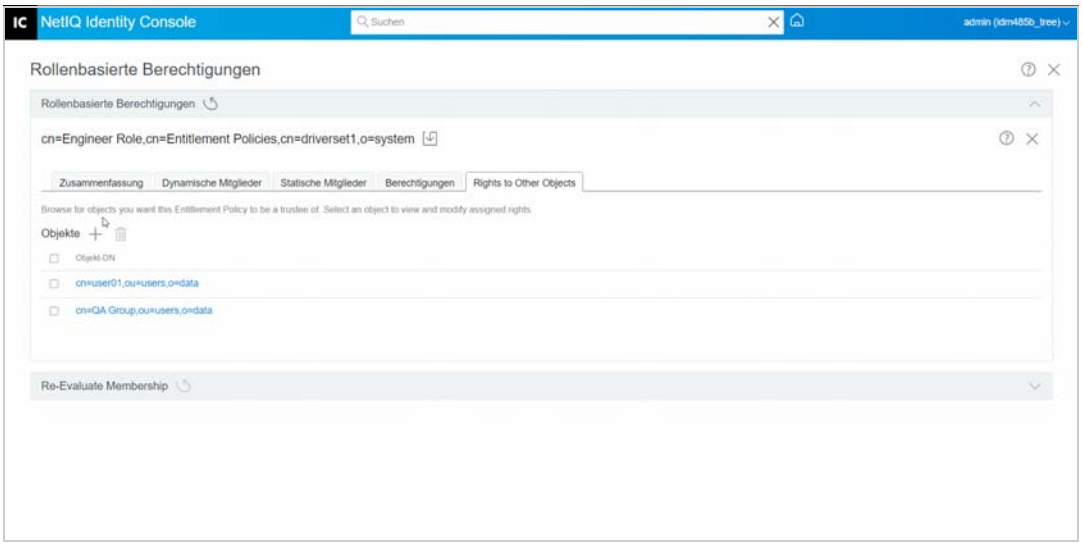


1c Um weitere Eigenschaften hinzuzufügen, klicken Sie auf +.

Die Seite **EIGENSCHAFTEN AUSWÄHLEN** wird angezeigt. Diese Seite enthält die Liste der Eigenschaften, die ein Objekt haben kann.

1d Klicken Sie auf **Fertig**.

Abbildung 33-4 *Wählen Sie „Eigenschaften“ aus*



2 (Optional) Verwenden Sie die Pfeile **Nach oben** und **Nach unten** ↑ ↓, um die Priorität der RBE-Richtlinien festzulegen.

Durch Festlegen der Priorität der Richtlinien können Berechtigungskonflikte zwischen mehreren Richtlinien aufgelöst werden. Die oberste Richtlinie hat höchste Priorität. Weitere Informationen hierzu finden Sie unter: „Priorität von RBE-Richtlinien festlegen“, auf Seite 219

Priorität von RBE-Richtlinien festlegen

Beim Erstellen von RBE-Richtlinien kann es vorkommen, dass sich Richtlinien für einen bestimmten Benutzer widersprechen.

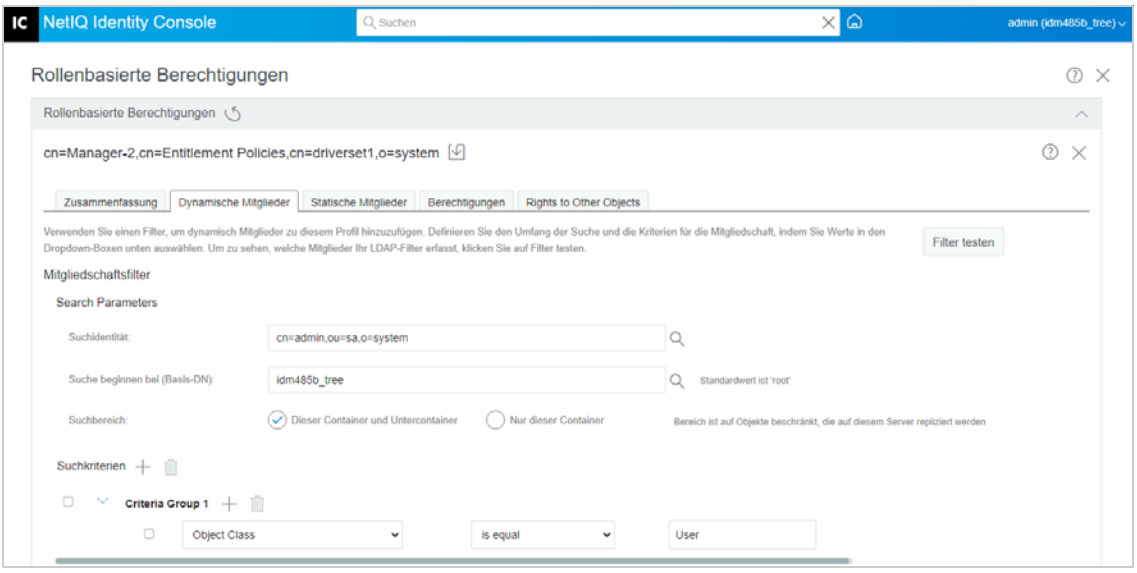
Die Reihenfolge, in der die RBE-Richtlinienn in der Liste aufgeführt sind, entspricht ihrer Priorität. Die Reihenfolge der Einträge in der Liste kann mit dem Auf- und Abwärtspfeil geändert werden.

- Diese Einstellung eignet sich beispielsweise dann, wenn ein Attribut für das verbundene System nur einen einzelnen Wert zulässt. Wenn zwei unterschiedliche RBE-Richtlinien einem Benutzer jeweils einen Wert für dieses Attribut zuweisen, wird dem Benutzer die Berechtigung aus der RBE-Richtlinie zugeteilt, die in der Liste am weitesten oben steht. Nehmen Sie als weiteres Beispiel an, dass in Ihrer Umgebung Berechtigungen verwendet werden, um Benutzer in hierarchischen Strukturen auf einem anderen System zu platzieren. Dabei möchten Sie sicherstellen, dass die Benutzer nur jeweils an einem Ort abgelegt werden und nicht an zwei Positionen gleichzeitig.
- Beachten Sie, dass diese Einstellung für jede Berechtigung in jedem Treiber einzeln gesetzt werden muss.
- In der Regel sollten Administrator- oder Managerrichtlinien weiter oben in der Liste stehen als Richtlinien für Endbenutzer oder einzelne Mitarbeiter. Gruppen mit enger gefassten Mitgliedschaftskriterien sollten höher als Gruppen mit breiter gefassten Mitgliedschaftskriterien eingeordnet werden.

So legen Sie die Priorität von RBE-Richtlinien fest:

1. Wählen Sie die Berechtigungsrichtlinie aus, die Sie hochstufen oder herabstufen möchten.
2. Verwenden Sie die Pfeile **Nach oben** und **Nach unten** , um die Priorität der RBE-Richtlinien festzulegen.

   Abbildung 33-5 *Richtlinienpriorität festlegen*

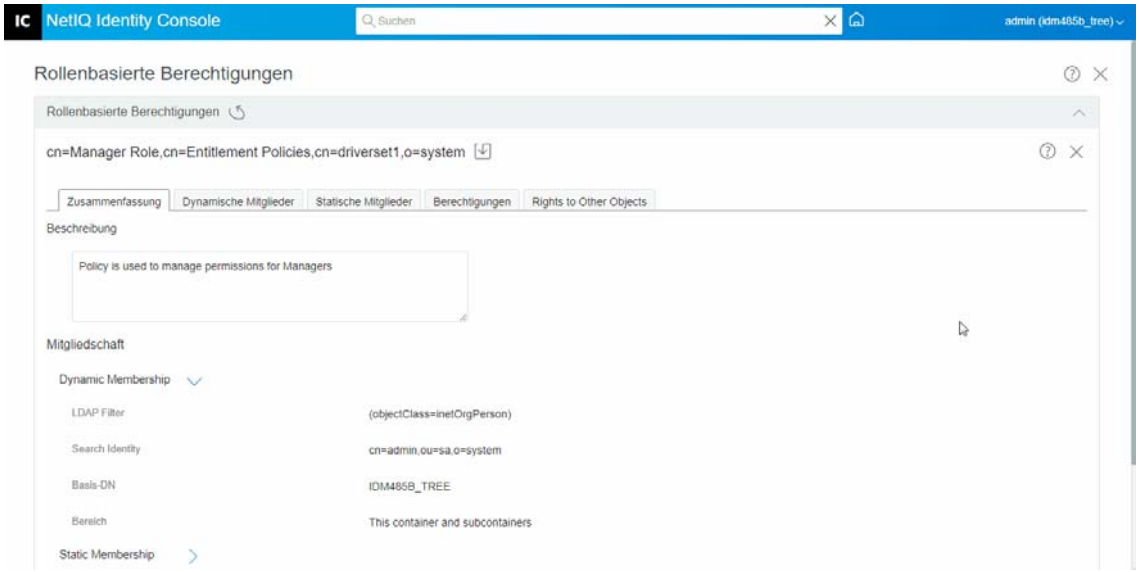


3. Klicken Sie auf die Schaltfläche „Speichern“ .

Die Zusammenfassung der Details zur Richtlinienmitgliedschaft wird auf der Registerkarte **Zusammenfassung** angezeigt.

4 Starten Sie den Treiber neu.

Abbildung 33-6 *Schließen und neu starten*



HINWEIS: Sie müssen den Treiber neu starten, damit die Änderungen wirksam werden.

Mitgliedschaft neu bewerten

Mit der Funktion **Rollenbasierte Berechtigungen** können Sie einer Benutzergruppe Berechtigungen für verbundene Systeme erteilen.

Beim Erstellen oder Bearbeiten einer RBE-Richtlinie muss die Mitgliedschaft jedes Benutzers neu geprüft werden, um festzustellen, ob Berechtigungen für verbundene Systeme erteilt, geändert oder entzogen werden müssen. Standardmäßig wird diese Überprüfung für jeden Benutzer einzeln durchgeführt, wenn ein Attribut für die Mitgliedschaft der Benutzer geändert oder ein Benutzer verschoben bzw. umbenannt wird. Dieses Standardverhalten minimiert zwar die Auslastung der Systemressourcen, führt aber gleichzeitig dazu, dass die Berechtigungen für einen bestimmten Benutzer erst eine Weile nach dem Ändern der RBE-Richtlinie erteilt, geändert oder entzogen werden.

Mit der Aufgabe „RBE-Richtlinien neu bewerten“, auf Seite 221 können Sie sicherstellen, dass die Berechtigungen aller Benutzer gleichzeitig aktualisiert werden, indem Sie angeben, welche Benutzer sofort neu bewertet werden sollen. Es wird empfohlen, diese Aufgabe bei jedem Erstellen oder Bearbeiten einer RBE-Richtlinie auszuführen.

In Versionen vor Identity Manager 3.6 wurde die Neubewertung von Mitgliedschaften für alle RBE-Richtlinien in einem Treibersatz und nicht nur für eine einzelne Berechtigungsrichtlinie ausgeführt. Mit Identity Manager 3.6 können Sie jedoch mit der Funktion **Bewerten** eine RBE-Richtlinie bewerten und deren Mitglieder über die Option **Hinzufügen** zur ausgewählten **Objektliste** hinzufügen. Wenn Sie eine Berechtigungsrichtlinie definiert und eine Mitgliedschaftsliste erstellt haben, wird neben dem Eintrag des ausgewählten Objekts die Überschrift **Bewerten Sie eine**

Berechtigungsrichtlinie, um ihre Mitglieder in die Liste aufzunehmen angezeigt. Wählen Sie die Richtlinie aus und klicken Sie dann auf das Symbol +, um die Richtlinienmitglieder zur Liste **Ausgewählte Objekte** hinzuzufügen. Sie können Mitglieder oder Objekte zur Liste **Ausgewählte Objekte** hinzufügen oder daraus entfernen.

Um die Systemressourcen möglichst zu schonen, sollten Sie alle Änderungen an den RBE-Richtlinien eines einzelnen Treibersatzes vornehmen, bevor Sie „RBE-Richtlinien neu bewerten“, auf Seite 221 verwenden.

HINWEIS: Die Neubewertung von Berechtigungen ist nur bei Berechtigungen für verbundene Systeme erforderlich. Wenn Identity Console-Rechte in einer RBE-Richtlinie geändert werden, wirken sich diese Änderungen sofort auf jeden Benutzer aus. Der Berechtigungs-Service-Treiber muss ausgeführt werden, damit Neubewertungen von Mitgliedschaften durchgeführt werden können.

RBE-Richtlinien neu bewerten

So bewerten Sie die Mitgliedschaft neu:

1. Klicken Sie auf **Mitgliedschaft neu bewerten** > **Treibersatz auswählen**.

   Eine Liste der erstellten Richtlinien wird angezeigt.

2. Wählen Sie die Richtlinie aus, die bewertet werden soll, und klicken Sie auf **Bewerten** Evaluate.

   Auf der Registerkarte **Objekte** werden die Benutzer angezeigt, die Teil der Gruppe sind.

3. (Optional) Klicken Sie zum Hinzufügen eines Benutzers auf +.

   Wenn Benutzer in der Liste fehlen und Sie bestimmte Benutzer hinzufügen möchten, können Sie diese Funktion **Hinzufügen** + verwenden.

4. (Optional) Um einen bestimmten Benutzer zu entfernen, klicken Sie auf 🗑.

   Wenn bestimmte Benutzer aus der Liste entfernt werden müssen, können Sie die Funktion **Löschen** 🗑 verwenden.

5. Klicken Sie auf die Schaltfläche „Mitgliedschaft neu bewerten“ ▷.

Abbildung 33-7 *Mitgliedschaft neu bewerten*