NetIQ® Identity Manager

Benutzerhandbuch zu den Identitätsanwendungen

März 2018

NetIQ

Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch und zur Bibliothek

In diesem Handbuch wird die Bedienung der NetIQ Identity Manager-Identitätsanwendungen für Endbenutzer und bestimmte Administratoren beschrieben, insbesondere das Dashboard und die Benutzeranwendung.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die mit Verwaltungskonzepten und der Implementierung eines sicheren, verteilten Verwaltungsmodells vertraut sein müssen.

Weitere Informationen in der Bibliothek

Weitere Informationen zur Identity Manager-Bibliothek finden Sie auf der Website der Identity Manager-Dokumentation.

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. Die Dokumentation für dieses Produkt steht auf der NetIQ-Website im HTML- und PDF-Format zur Verfügung. Eine Anmeldung ist nicht erforderlich, um auf diese Dokumentationsseite zuzugreifen. Wenn Sie uns einen Verbesserungsvorschlag für die Dokumentation mitteilen möchten, nutzen Sie die Schaltfläche **Kommentar hinzufügen**, die unten auf jeder Seite der unter www.netiq.com/documentation veröffentlichten HTML-Version 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

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

Willkommen bei Identity Manager

NetIQ Identity Manager ist eine Systemsoftware, mit der Ihre Organisation die Zugriffsanforderungen der Benutzer-Community sicher verwalten kann. Wenn Sie Mitglied dieser Benutzer-Community sind, haben Sie durch Identity Manager verschiedene Vorteile. So ermöglicht Identity Manager Ihrer Organisation unter anderem Folgendes:

- Benutzern bereits ab dem ersten Tag Zugriff auf benötigte Informationen (z. B. Gruppenorganigramme, White Pages von Abteilungen oder Suche nach Mitarbeitern) sowie Rollen und Ressourcen (z. B. Geräte oder Konten auf internen Systemen) gewähren
- Mehrere Passwörter für eine einmalige Anmeldung auf allen Systemen synchronisieren
- Zugriffsrechte bei Bedarf sofort ändern oder entziehen (z. B. wenn eine Person zu einer anderen Gruppe wechselt oder die Organisation verlässt)
- Die Einhaltung von behördlichen Vorschriften gewährleisten

Lesen Sie zuerst diesen Teil, um eine Einführung in die Identity Manager-Identitätsanwendungen und deren Verwendung zu erhalten. Dieses Handbuch unterstützt die folgenden Arten von Online-Aktivitäten in Ihrer Organisation:

- Zugeordnete Online-Identität für Organisationsressourcen verwalten
- Zugriff auf Organisationsrollen anzeigen oder bearbeiten
- Zugriffsanforderungen auf Ressourcen und Rollen genehmigen
- Zugeordnete Berechtigungen für Software-Anwendungen und andere Ressourcen verwalten, die Ihre Organisation den Mitgliedern Ihrer Organisation bereitstellt

1 Einführung

In diesem Abschnitt wird erläutert, wie Sie die Arbeit mit den Identitätsanwendungen beginnen. Es werden u. a. folgende Themen erläutert:

1.1 Grundlagen von Rollen und Ressourcen

In den Identitätsanwendungen stellt eine **Berechtigung** den Zugriff dar, den ein Benutzer oder eine Gruppe von Benutzern auf eine Rolle oder Ressource erhält. Eine **Rolle** definiert eine Reihe von Berechtigungen, die in Beziehung zu einem oder mehreren Zielsystemen oder Anwendungen stehen. Eine Benutzeradministratorrolle ist beispielsweise berechtigt, das Passwort eines Benutzers zurückzusetzen, während eine Systemadministratorrolle in der Lage ist, einen Benutzer einem bestimmten Server zuzuweisen. Eine **Ressource** ist eine digitale Entität, wie z. B. ein Benutzerkonto, ein Computer oder eine Datenbank, auf die ein Geschäftsbenutzer zugreifen muss.

1.2 Grundlagen der Identitätsanwendungen

Die Identity Manager-Anwendungen bestehen aus einer Reihe miteinander verbundener browsergestützter Webanwendungen. Ihre Organisation verwaltet hiermit die Benutzerkonten und Berechtigungen für die zahlreichen verschiedenen Rollen und Ressourcen, die den Benutzern zur Verfügung stehen. Sie können die Identitätsanwendungen mit Selbstbedienungssupport für Ihre Benutzer einrichten, z. B. zum Anfordern von Rollen oder zum Ändern der Passwörter. Außerdem können Sie Workflows einrichten, mit denen sich die Rollen und Ressourcen noch effizienter verwalten und zuweisen lassen.

1.3 Erläuterungen zum Identity Manager-Dashboard

Das Identity Manager-Dashboard fungiert als primäres Zugangsportal zu den Identitätsanwendungen. Das Dashboard umfasst ein oder auch mehrere Widgets mit Kurzinformationen zu bestimmten Aktivitäten. Im Dashboard können Sie die folgenden Aktivitäten ausführen:

- Profileinstellungen und Passwörter verwalten.
- Ihre Organigrammdetails abrufen.
- Aufgaben prüfen und ausführen, z. B. Zugriffsanforderungen der Benutzer.
- Berechtigungen für Rollen, Ressourcen oder Prozesse anfordern.

- Status und Verlauf der Berechtigungsanforderungen prüfen.
- Andere Benutzer in der Organisation suchen.
- Das Dashboard personalisieren. Sie können Widgets hinzufügen und nach Wunsch anordnen.
- Einen beliebigen Benutzer als Ihre Vertretung im System festlegen.
- Ihre Aufgaben an andere Benutzer im System delegieren.

Mit den entsprechenden **Berechtigungen** können Sie die folgenden Aufgaben ausführen:

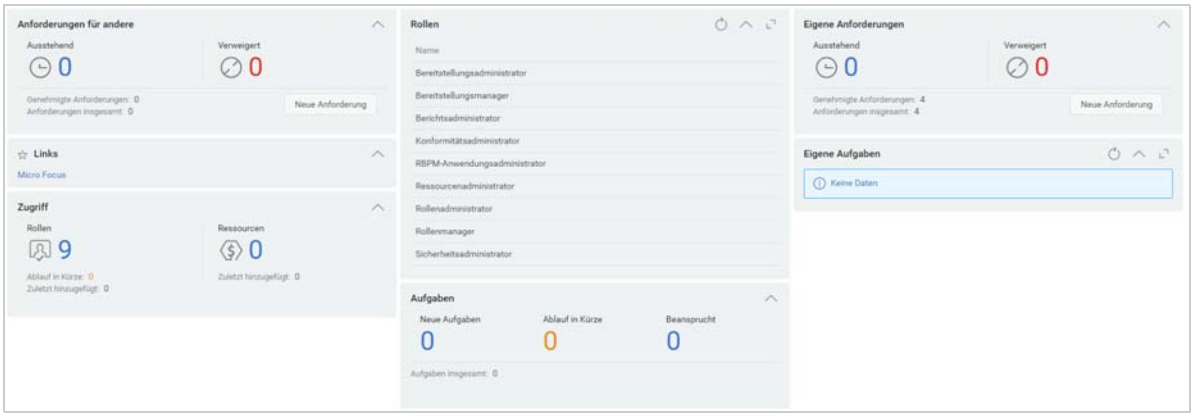
- Benutzerprofile erstellen und bearbeiten.
- Organigrammdetails anderer Benutzer abrufen.
- Teams aus Benutzern und Gruppen erstellen und bearbeiten, die Bereitstellungsanforderungen und Genehmigungsaufgaben in Zusammenhang mit den Teams abgeben können.
- Berechtigungen im Namen anderer Benutzer in der Organisation abrufen oder entziehen.

1.4 Übersicht über das Dashboard

Das Dashboard bietet Kurzinformationen zu Ihren Aufgaben, Berechtigungen und Anforderungen in Form von Widgets. Mit einem einfachen Klick navigieren Sie zu den jeweiligen Seiten oder Anwendungen. Außerdem haben Sie die Möglichkeit, Widgets am Dashboard hinzuzufügen, neu zu positionieren und zu konfigurieren. Weitere Informationen zum Personalisieren des Dashboards finden Sie unter Teil II, „Anpassen des Dashboards“, auf Seite 27.

Das nachfolgende Beispiel-Dashboard zeigt die standardmäßigen Widget-Optionen im Dashboard.

Abbildung 1-1 *Beispiel für ein persönliches Dashboard*



Im Identity Manager-Dashboard verwalten Sie verschiedene Aktivitäten in Identity Manager. Die folgenden Seiten helfen Ihnen, Ihre Aufgaben und Aktivitäten zu verwalten:

Anwendung

Hier finden Sie eine Liste aller Anwendungen, die für Sie bereitgestellt wurden. Die Liste enthält Standard-Links zu verschiedenen Bereichen, die die grundlegenden Aufgaben in Identity Manager optimieren. Weitere Informationen finden Sie unter Abschnitt 1.4.1, „Erläuterungen zur Seite „Anwendungen““, auf Seite 15.

Aufgaben

Hier finden Sie alle Aufgaben, für die eine Aktion aussteht. Mit der entsprechenden Rolle können Sie die Aufgaben anderer Benutzer abrufen. Beispiel: Team-Manager.

Zugriff

Hier können Sie Berechtigungen abrufen oder anfordern. Unter **Anforderungsverlauf** finden Sie den Status der angeforderten Berechtigungen. Diese Seite zeigt Ihre Anforderungen und deren Status.

Personen

Hier können Sie andere Benutzer oder Gruppen im System sowie das **Organigramm** anderer Benutzer abrufen. So wird erkennbar, wie diese Benutzer und Gruppen zusammenhängen.

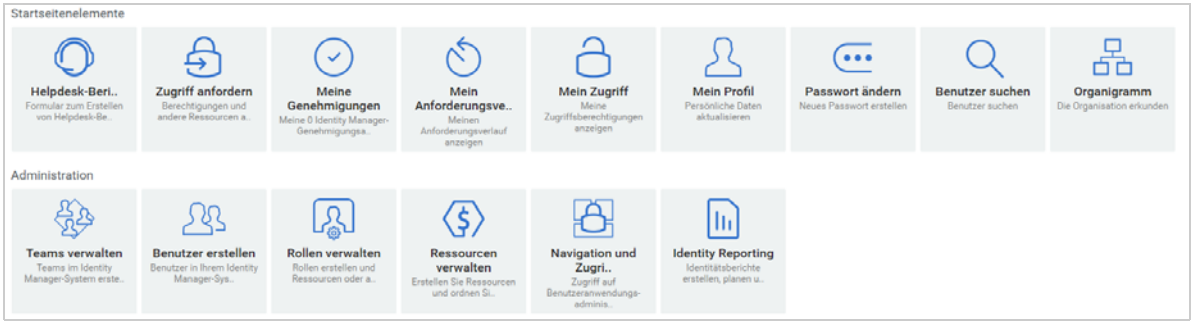
Administration

Hier können Sie Rollen, Ressourcen, den Berechtigungsabgleich und die zugehörigen Konfigurationen abrufen. Diese Option wird nur für Administratoren angezeigt. Weitere Informationen zu Administrationsaufgaben finden Sie unter Administration der Identitätsanwendungen im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

1.4.1 Erläuterungen zur Seite „Anwendungen“

Die zweite wichtige Ansicht im Dashboard ist die Seite **Anwendungen** (Abbildung 1-2), auf der sich Standardlinks zu verschiedenen Bereichen befinden, die die grundlegenden Aufgaben von Endbenutzern und Administratoren in Identity Manager erleichtern.

Abbildung 1-2 *Beispiel für die Anwendungsseite im Dashboard*



Standardmäßig wird **Helpdesk-Ticket** auf der Seite **Anwendungen** angezeigt. Mit dieser Option können Sie ein Ticket für den Helpdesk erstellen.

Ihr Identitätsadministrator passt die Seite **Anwendungen** so an, dass Kacheln mit Links zu häufig angeforderten Ressourcen oder zu häufig aufgerufenen Anwendungen angezeigt werden.

Einige Kacheln auf dieser Seite sind nur für Benutzer mit Administratorrolle in den Identitätsanwendungen sichtbar. Eine Person, die Rollen erstellen oder bearbeiten kann, sieht beispielsweise die Kacheln **Benutzer erstellen** und **Rollen verwalten** (oder ähnliche Kacheln).

Weitere Informationen zur Bedienung des Dashboards finden Sie unter Kapitel IV, „Verwalten von Benutzern, Gruppen und Teams“, auf Seite 63 und in der Hilfe (?) im Dashboard.

1.5 Erläuterung von Jobs

Auf der Seite **Aufgaben** können Sie Aktionen für die aufgeführten Aufgaben genehmigen oder ablehnen. Standardmäßig werden alle **Selbst**-Aufgaben angezeigt. Mit der entsprechenden Rolle können Sie die Aufgaben anderer Benutzer abrufen. Sollen die Aufgaben anderer Benutzer angezeigt werden, klicken Sie auf **Sonstige**.

- Durchsuchen Sie Ihre Aufgaben mit den Filtern **Neu zugewiesene Aufgaben**, **Zurückgegebene Aufgaben** oder **Delegierte Aufgaben**. Mit dem Filter **Delegierte Aufgabe** für **Selbst** werden nur die Aufgaben angezeigt, die an Sie delegiert wurden.
- Wenn Sie Administrator sind, können Sie die Aufgaben auch mit **Mir zugewiesen** und **Empfänger als Ich** filtern.
- Die Aufgaben anderer Personen durchsuchen Sie anhand der Filter **Zurückgegebene Aufgaben**, **Neu zugewiesene Aufgaben** oder **Delegierte Aufgaben** . Mit dem Filter **Delegierte Aufgaben** für **Andere** werden alle Aufgaben angezeigt, die an andere Benutzer im System delegiert wurden.
- Sie können die Aufgabensuche auch basierend auf den im System vorhandenen Aufgaben verfeinern:
  1. Wählen Sie aus.
  2. (Bedingt) Geben Sie zur Anzeige der für einen bestimmten Zeitraum erstellten Aufgaben den Zeitraum in **Wochen**, **Tage** oder **Stunden** an.
  3. (Bedingt) Geben Sie den Aufgabenstatus an, den Sie filtern möchten.
  4. Klicken Sie auf **Filter**.
- Als Helpdesk-Benutzer erhalten Sie mit **Helpdesk-Aufgaben** die verfeinerte Liste. Weitere Informationen zum Verwalten der Helpdesk-Aufgaben finden Sie in der Dashboard-Hilfe.

Weitere Informationen zum Verwalten von Aufgaben finden Sie unter Kapitel 5, „Verwalten Ihrer Aufgaben“, auf Seite 43.

1.6 Typische Verwendungsmöglichkeiten für die Identitätsanwendungen

Nachfolgend wird anhand einiger Beispiele erläutert, wie die Identitätsanwendungen in einer Organisation in der Regel verwendet werden.

1.6.1 Wie funktioniert die Identitätsselbstbedienung?

- Ella (eine Endbenutzerin) hat ihr Passwort vergessen und stellt dieses bei der Anmeldung mithilfe der Identitätsselbstbedienung wieder her.

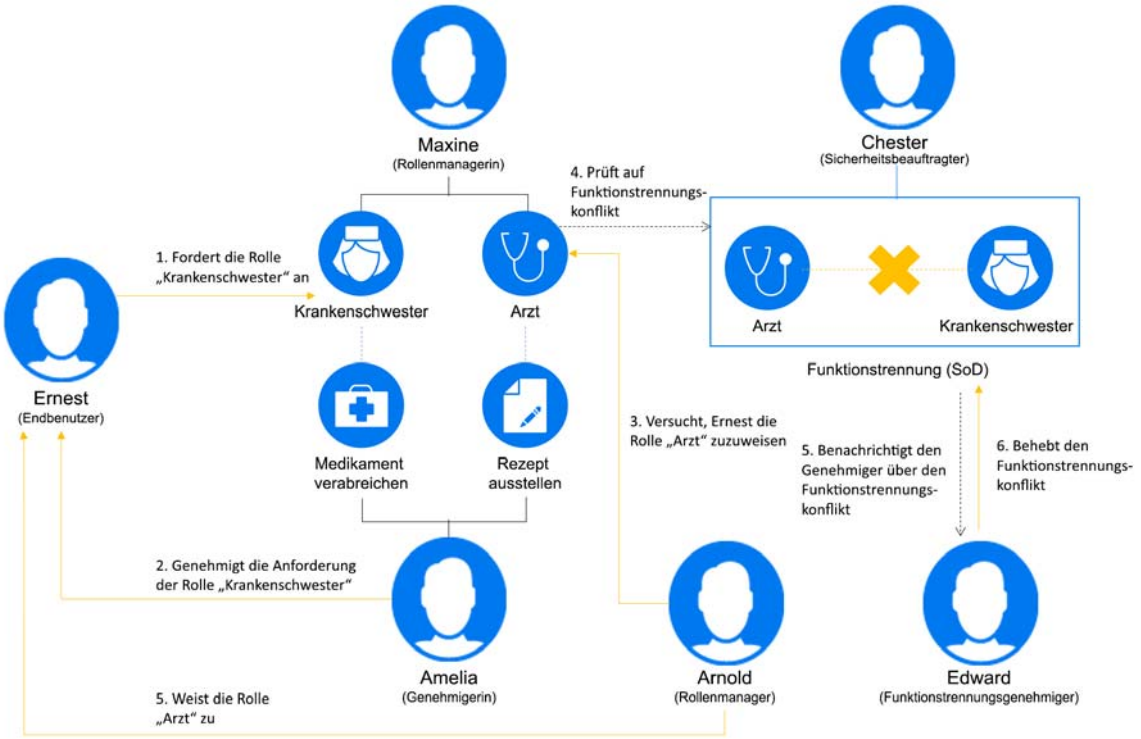
Standardmäßig bietet Identity Manager die Komponente Self Service Password Reset (SSPR), damit Benutzer ihre Passwörter ändern bzw. zurücksetzen können. In den Identitätsanwendungen können jedoch auch andere Methoden zur Verwaltung vergessener Passwörter verwendet werden.

- Erik (ein Endbenutzer) führt eine Suche nach allen Mitarbeitern an seinem Standort durch, die Deutsch sprechen.
- Eduardo (ein Endbenutzer) durchsucht das Organigramm der Organisation, findet Ella und klickt auf das Email-Symbol, um ihr eine Nachricht zu senden.

1.6.2 Wie funktionieren Rollen und Ressourcen?

Das folgende Beispiel erläutert den Ablauf von Rollen- und Ressourcenanforderungen im System:

Abbildung 1-3 *Beispielszenario des Rollenzuweisungsablaufs*



- Maxine (eine Rollenmanagerin) erstellt die Geschäftsrollen „Krankenschwester“ und „Arzt“ sowie die IT-Rollen „Medikament verwalten“ und „Rezept ausstellen“. Maxine erstellt mehrere Ressourcen, die für diese Rollen erforderlich sind, und verknüpft die Ressourcen mit den Rollen.
- Maxine (eine Rollenmanagerin) definiert eine Beziehung zwischen den Rollen „Krankenschwester“ und „Medikament verabreichen“ und gibt an, dass die Rolle „Krankenschwester“ die Rolle „Medikament verabreichen“ enthält. Maxine definiert außerdem eine Beziehung zwischen den Rollen „Rezept ausstellen“ und „Arzt“ und gibt an, dass die Rolle „Arzt“ die Rolle „Rezept ausstellen“ enthält.
- Chester (ein Sicherheitsbeauftragter) definiert eine Funktionstrennungsbeschränkung, die angibt, dass ein potenzieller Konflikt zwischen den Rollen „Arzt“ und „Krankenschwester“ besteht. Dies bedeutet, dass für gewöhnlich ein Benutzer nicht gleichzeitig beiden Rollen zugewiesen sein darf. In einigen Fällen kann es vorkommen, dass eine Person, die eine

Rollenzuweisung anfordert, diese Beschränkung aufheben möchte. Damit eine Funktionstrennungsausnahme definiert werden kann, muss die Person, die eine Zuweisung anfordert, eine Begründung angeben.

- Ernest (ein Endbenutzer) durchsucht eine Liste mit Rollen, die ihm zur Verfügung stehen, und fordert eine Zuweisung zur Rolle „Krankenschwester“ an.
- Amelia (eine Genehmigerin) erhält eine Benachrichtigung über eine Genehmigungsanforderung per Email (die eine URL enthält). Sie klickt auf den Link, woraufhin ein Genehmigungsformular geöffnet wird, und sie genehmigt die Anforderung.
- Arnold (ein Rollenmanager) fordert an, dass Ernest die Rolle „Arzt“ zugewiesen wird. Er wird benachrichtigt, dass ein potenzieller Konflikt zwischen der Rolle „Arzt“ und der Rolle „Krankenschwester“ besteht, die Ernest bereits zugewiesen wurde. Er liefert eine Begründung für eine Ausnahme von der Funktionstrennungsbeschränkung.
- Edward (ein Funktionstrennungsgenehmiger) empfängt per Email eine Benachrichtigung über einen Funktionstrennungskonflikt. Er genehmigt Arnolds Anforderung auf Aufhebung der Funktionstrennungsbeschränkung.
- Amelia (eine Genehmigerin) erhält per Email eine Benachrichtigung über eine Genehmigungsanforderung für die Rolle „Arzt“. Sie genehmigt Arnolds Anforderung auf Zuweisung von Ernest zur Rolle „Arzt“.
- Bill (ein Rollen-Auditor) liest den Bericht zu Verletzungen und Ausnahmen bei der Funktionstrennung und sieht, dass Ernest sowohl der Rolle „Arzt“ als auch „Krankenschwester“ zugewiesen wurde. Darüber hinaus stellt er fest, dass Ernest die mit diesen Rollen verknüpften Ressourcen zugewiesen wurden.

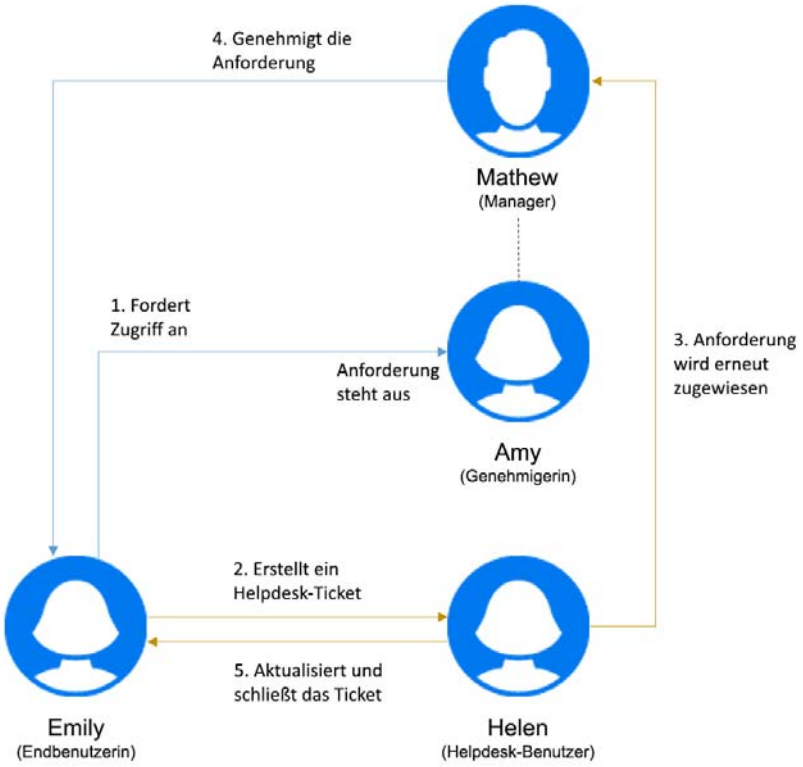
1.6.3 Wie funktionieren Prozessanforderungen?

- Ernie (ein Endbenutzer) durchsucht eine Liste mit Ressourcen, die ihm zur Verfügung stehen, und fordert Zugriff auf das Siebel*-System an.
- Amy (eine Genehmigerin) erhält eine Benachrichtigung über eine Genehmigungsanforderung per Email (die eine URL enthält). Sie klickt auf den Link, woraufhin ein Genehmigungsformular geöffnet wird, und sie genehmigt die Anforderung.
- Ernie prüft den Status der von ihm eingereichten Anforderung des Zugriffs auf das Siebel-System (die jetzt zur Genehmigung an eine zweite Person weitergeleitet wurde). Er sieht, dass die Anforderung noch bearbeitet wird.
- Amy geht in Urlaub und gibt an, dass sie vorübergehend nicht verfügbar ist. Während ihrer Abwesenheit werden ihr keine neuen Genehmigungsaufgaben zugeteilt.
- Amy öffnet ihre Genehmigungsliste, sieht, dass sie vor ihrem Urlaub nicht mehr alle Anforderungen bearbeiten kann, und leitet einige davon an Kollegen weiter.
- Pat (ein Verwaltungsassistent, der als Vertreter von Amy agiert) öffnet die Aufgabenliste von Amy und führt eine Genehmigungsaufgabe für sie durch.
- Max (ein Vorgesetzter) prüft die Aufgabenlisten von Mitarbeitern seiner Abteilung. Er weiß, dass Amy in Urlaub ist. Daher teilt er Aufgaben anderen Mitarbeitern seiner Abteilung zu.
- Max initiiert eine Anforderung für ein Datenbankkonto für einen Mitarbeiter seiner Abteilung, dessen direkter Vorgesetzter er ist.
- Max ernennt Dan zum autorisierten Delegierten von Amy.
- Dan (jetzt ein delegierter Genehmiger) empfängt Amys Aufgaben, während sie abwesend ist.
- Max beschäftigt einen Praktikanten, der nicht in das HR-System eingegeben werden soll. Der Systemadministrator erstellt einen Benutzerdatensatz für den Praktikanten und fordert für ihn die Zugriffsberechtigung für Notes, Active Directory* und Oracle* an.

1.6.4 Wie funktioniert der Helpdesk?

Das folgende Beispiel erläutert den Ablauf eines Helpdesk-Tickets im System:

Abbildung 1-4 *Beispiel für Helpdesk*



- Emily (eine Endbenutzerin) hat den Zugriff auf einen Bürodrucker angefordert. Diese Anforderung war lange Zeit ausstehend. Darum hat sie ein Helpdesk-Ticket erstellt.
- Helen (eine Helpdesk-Benutzerin) erhält eine Benachrichtigung über das Helpdesk-Ticket in ihrer Aufgabenliste.
- Helen analysiert das Problem und stellt fest, dass die Anforderung Amy (einer Genehmigerin) zugewiesen wurde.
- Diese Anforderung wird im System als ausstehend geführt, weil Amy abwesend ist.
- Helen besitzt die Berechtigung, Aufgabenanforderungen neu zuzuweisen. Sie weist diese Anforderung Mathew (Amys Manager) neu zu.
- Mathew prüft die Anforderung und genehmigt sie. Emily kann auf den Bürodrucker zugreifen.
- Helen aktualisiert und schließt das Helpdesk-Ticket.

2 Zugriff auf die Identitätsanwendungen

Der Zugriff auf die Identitätsanwendungen, z. B. auf das Dashboard, erfolgt in einem Webbrowser. Identity Manager unterstützt alle gängigen Browser-Versionen. Fragen Sie Ihren Systemadministrator nach einer Liste der unterstützten Browser oder bitten Sie ihn um Hilfe bei der Installation eines Browsers. Ihre Organisation sollte Ihnen die URL und den Berechtigungsnachweis für den Zugriff auf die Anwendungen bereitstellen.

2.1 Überlegungen beim Zugriff auf die Identitätsanwendungen

Bevor Sie auf das Dashboard oder auf eine der anderen Identitätsanwendungen zugreifen, beachten Sie die folgenden Überlegungen:

- Sie müssen Cookies und JavaScript* in Ihrem Webbrowser aktivieren.
- Wenn Sie Internet Explorer verwenden, müssen Sie mindestens die Sicherheitsstufe **Mittel** einstellen. Außerdem sollten Sie die Option **Bei jedem Zugriff auf die Seite** unter **Extras > Internetoptionen > Allgemein, Temporäre Internetdateien > Einstellungen > Neuere Versionen der gespeicherten Seiten suchen** auswählen. Wenn diese Option nicht ausgewählt ist, werden möglicherweise manche Schaltflächen nicht richtig angezeigt.
- Wenn Sie die Identity Manager-Benutzeranwendung bereits verwendet haben, sollten Sie das Dashboard mit der gleichen Benutzername-Passwort-Kombination aufrufen können.
- Der Name des Kontos für den Zugriff auf die Identitätsanwendungen darf keines der folgenden Zeichen enthalten:

  `\ /, * ? . $ # +`

- Wenn Sie sich nicht anmelden können, klicken Sie auf **Passwort vergessen?**. Weitere Informationen finden Sie unter Abschnitt 2.4.1, „Vergessen des Passworts“, auf Seite 24.
- Wenn die erste Seite Ihrer Identity Manager-Benutzerschnittstelle anders aussieht, wurde die Anwendung vermutlich an die Anforderungen Ihrer Organisation angepasst. Bei Ihrer Arbeit werden Sie möglicherweise feststellen, dass auch andere Funktionen der Identitätsanwendungen geändert wurden.

  Fragen Sie in diesem Fall Ihren Systemadministrator, inwieweit sich Ihre angepassten Identitätsanwendungen von der in diesem Handbuch beschriebenen Standardkonfiguration unterscheiden.

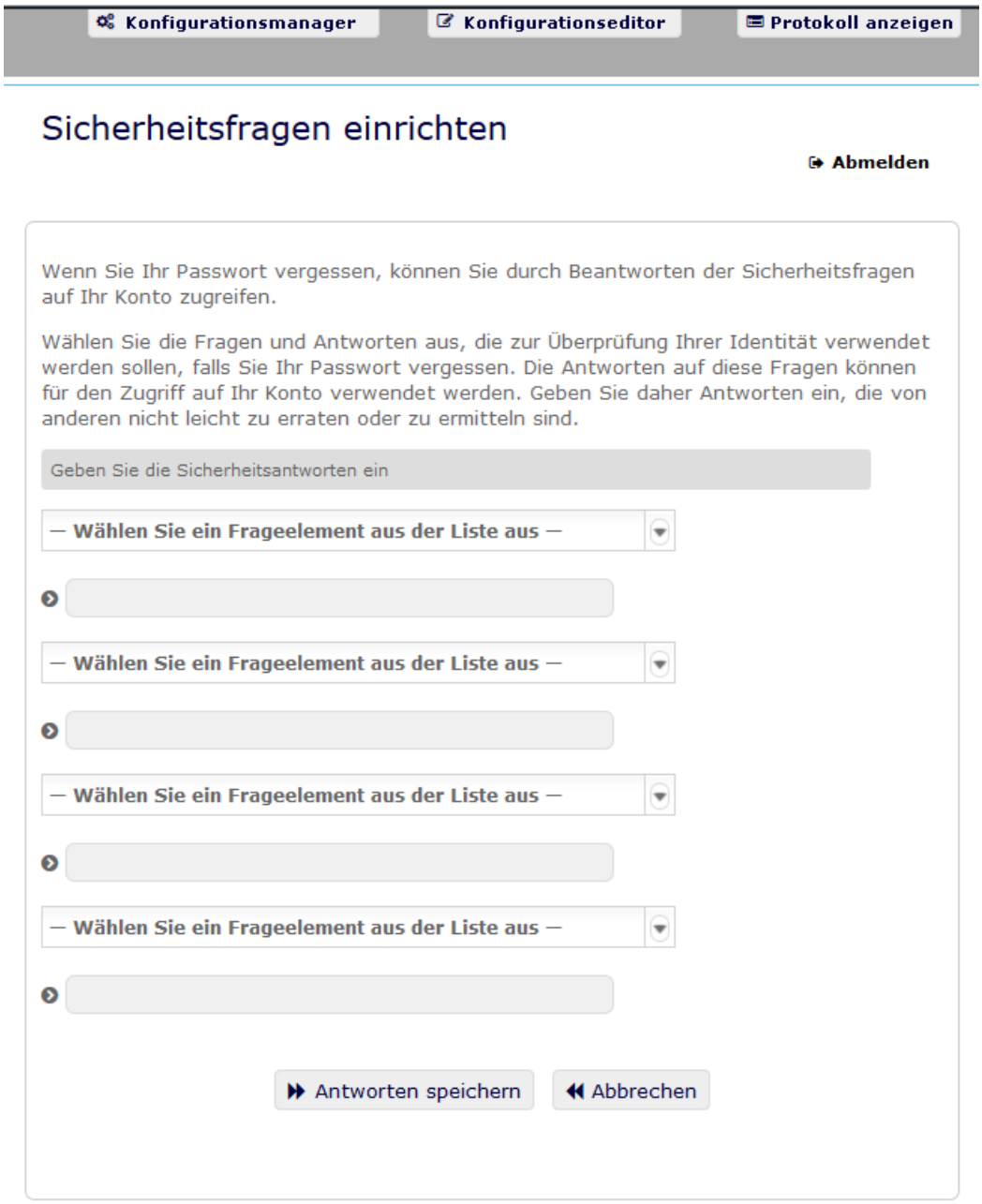
2.2 Erstmalige Anmeldung

Sie können sich nur als autorisierter Benutzer bei den Identitätsanwendungen anmelden, z. B. beim Dashboard. Wenn Sie noch keinen Benutzernamen und kein Passwort für die Anmeldung haben, wenden Sie sich an den Systemadministrator.

Wenn Sie sich erstmalig bei den Identitätsanwendungen anmelden, fordert Identity Manager Sie auf, Sicherheitsparameter für Ihr Konto festzulegen, mit denen Sie Ihr Passwort in Zukunft bei Bedarf zurücksetzen können. Falls Sie Ihr Passwort vergessen haben und versuchen, es bei der nächsten Anmeldung zurückzusetzen, fragt Sie Identity Manager nach den hier eingegebenen Antworten auf diese Sicherheitsfragen. Stimmen Ihre Antworten dann mit den auf dieser Seite gespeicherten Eingaben überein, können Sie Ihr Passwort zurücksetzen.

So richten Sie die Sicherheitsfragen bei der ersten Anmeldung ein:

1. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie dann auf **Anmelden**.
2. Über die Anmeldeseite werden Sie automatisch auf die Seite **Sicherheitsabfrage** weitergeleitet.
3. Geben Sie die Fragen und Antworten für die Sicherheitsfragen an.



4 Klicken Sie auf **Antworten speichern**. Sie gelangen wieder zum Dashboard zurück.

2.3 Reaktion auf die Nachfrage nach einem bevorzugten Gebietsschema

Wenn Sie bei der Anmeldung aufgefordert werden, ein bevorzugtes Gebietsschema auszuwählen, hat Ihr Administrator die Identitätsanwendung so konfiguriert, dass eine Sprachprüfung auf den Browsern der Benutzer ausgeführt wird. Dies ist ggf. notwendig, damit Ihre eingegebenen Inhalte in einer unterstützten Sprache angezeigt werden können.

Wenn Sie aufgefordert werden, ein Gebietsschema anzugeben, öffnen Sie die Liste **Verfügbare Gebietsschemen**, wählen Sie ein Gebietsschema aus und klicken Sie auf **Hinzufügen**. Weitere Informationen finden Sie unter.

2.4 Fehlersuche bei Anmeldeproblemen

In diesem Abschnitt finden Sie Lösungen für die folgenden häufigen Anmeldeprobleme:

- Abschnitt 2.4.1, „Vergessen des Passworts“, auf Seite 24
- Abschnitt 2.4.2, „Probleme bei der Anmeldung“, auf Seite 24
- Abschnitt 2.4.3, „Frage nach weiteren Informationen“, auf Seite 25

2.4.1 Vergessen des Passworts

Wenn Sie Ihr Passwort vergessen haben, kann Ihnen der Link **Passwort vergessen?** möglicherweise weiterhelfen. Wenn Sie aufgefordert werden, sich anzumelden, wird dieser Link standardmäßig auf der Seite angezeigt. Sie können diesen Link nutzen, wenn Ihr Systemadministrator die entsprechende Passwortrichtlinie für Sie eingerichtet hat.

1. Wenn Sie aufgefordert werden, sich anzumelden, klicken Sie auf den Link **Passwort vergessen?**.
2. Geben Sie Ihren Benutzernamen ein und klicken Sie auf **Senden**.

   Wenn Identity Manager keine Passwortrichtlinie für Sie findet, wenden Sie sich an den Systemadministrator.
3. Beantworten Sie die angezeigten Sicherheitsfragen. Sie werden von Identity Manager nur nach den konfigurierten Antworten gefragt. Stimmen Ihre Antworten mit den zuvor auf dieser Seite gespeicherten Eingaben überein, können Sie Ihr Passwort zurücksetzen. Klicken Sie auf **Senden**. Beispiel:

   Wenn Sie die Sicherheitsabfragen beantwortet haben, erhalten Sie Hilfe zu Ihrem Passwort. Je nach Konfiguration der Passwortrichtlinie durch den Systemadministrator stehen folgende Möglichkeiten zur Verfügung:

   - Empfang einer Email mit Ihrem Passwort dazu
   - Sie werden aufgefordert, das Passwort zurückzusetzen.

2.4.2 Probleme bei der Anmeldung

Wenn Sie sich nicht anmelden können, vergewissern Sie sich, dass Sie den Benutzernamen und das Passwort korrekt eingegeben haben (Rechtschreibung, Groß-/Kleinschreibung usw.). Wenn Sie weiterhin Probleme haben, wenden Sie sich an den Systemadministrator. Es ist hilfreich, wenn Sie Details zu Ihrem Problem angeben können (z. B. die Fehlermeldung).

2.4.3 Frage nach weiteren Informationen

Sie werden möglicherweise nach weiteren Informationen gefragt, sobald Sie sich angemeldet haben. Auch dies hängt davon ab, wie der Systemadministrator Ihre Passwortrichtlinie (sofern vorhanden) eingerichtet hat. Beispiel:

- Falls dies Ihre erste Anmeldung ist, werden Sie zur Einrichtung Ihrer Sicherheitsfragen und -antworten aufgefordert
- Wenn Ihr Passwort abgelaufen ist, werden Sie aufgefordert, es zurückzusetzen

2.5 Abmelden

Wenn Sie Ihre Arbeit im Dashboard und in anderen Identitätsanwendungen beendet haben, sollten Sie sich abmelden. Klicken Sie oben rechts im Dashboard auf Ihren Benutzernamen und wählen Sie **Abmelden**.

Anpassen des Dashboards

Die Identitätsanwendungen bieten viele Optionen zum Ändern der Anzeige des Dashboards und zum Speichern des Dashboards als personalisierte Ansicht. Beispielsweise können Sie Widgets hinzufügen und wunschgemäß neu positionieren. Die Widget-Felder lassen sich auch konfigurieren und personalisieren. In diesem Dokument werden die verschiedenen Optionen zur Personalisierung des Dashboards erklärt.

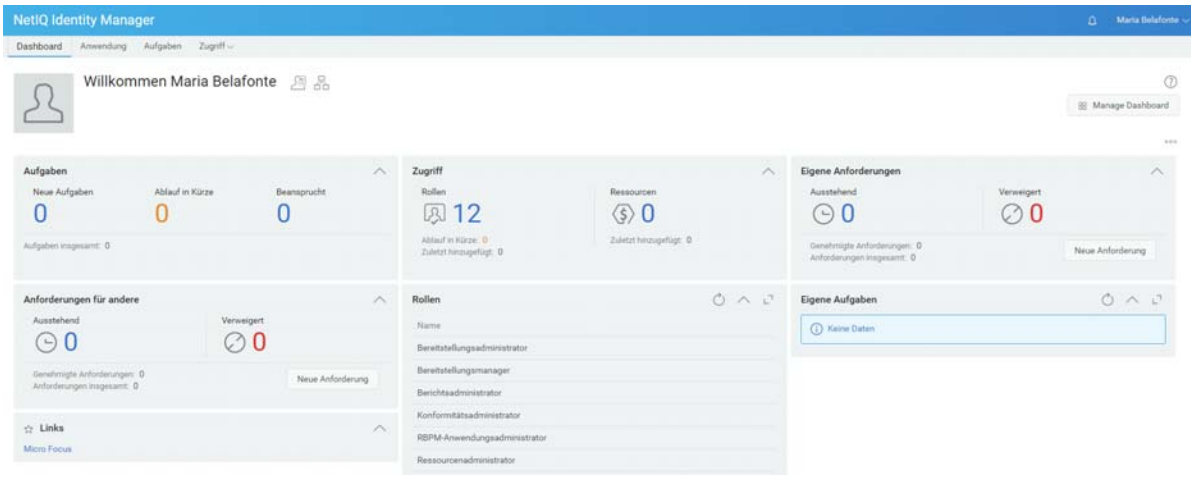
3 Verwalten von Widgets und Layouts

Widgets sind Dashboard-Objkete, die spezielle Details eines Benutzers für eine bestimmte Aktivität zur Verfügung stellen sollen. Das Aufgaben-Widget beispielsweise bietet Details zu neuen Aufgaben, beanspruchten Aufgaben oder Aufgaben, die bald ablaufen. Es sind viele andere ähnliche Widgets verfügbar, die am Dashboard konfiguriert werden können.

Administratoren, die Zugriff auf die Seite **Einstellungen** haben, können Widgets für einen Benutzer, eine Gruppe, einen Container oder eine Rolle über **Ihre ID > Einstellungen > Dashboard-Widgets** bereitstellen.

Wechseln Sie zum Personalisieren Ihres Dashboards zu **Dashboard** und klicken Sie auf ∘∘∘.

Abbildung 3-1 *Personalisieren des Dashboards*



Personalisieren Sie Ihr Dashboard mit den folgenden Optionen:

Abbildung 3-2 *Personalisierungsoptionen*

Widgets

Mit dieser Option fügen Sie Widget zum Dashboard hinzu. Siehe Abschnitt 3.3, „Hinzufügen eines Widgets“, auf Seite 31.

Layout

Ermöglicht Ihnen, das Dashboard-Layout zu ändern. Siehe Abschnitt 3.2, „Ändern des Dashboard-Layouts“, auf Seite 30.

Abbrechen

Bricht alle am Dashboard vorgenommenen Änderungen ab.

Speichern

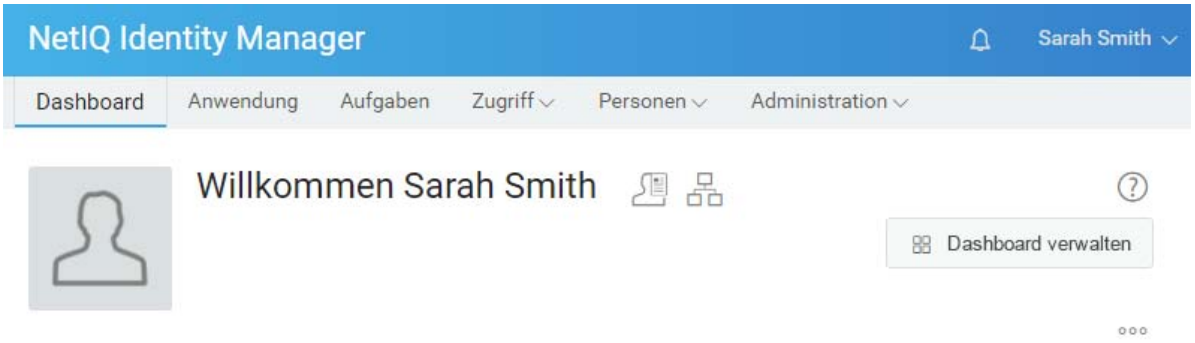
Speichert Ihre Änderungen und wendet sie auf Ihr Dashboard an.

3.1 Verwalten des globalen Dashboards

Das globale Dashboard umfasst mehrere Widgets, die im Dashboard aller Benutzer im System angezeigt werden. Die Benutzer können diese Widgets gemäß ihren Zugriffsberechtigungen abrufen, die ihnen durch einen Administrator zugewiesen wurden. Mit der Option **Dashboard verwalten** können Sie Widgets im globalen Dashboard einfügen, bearbeiten oder entfernen.

HINWEIS: Die Option **Dashboard verwalten** können Sie nur dann verwenden, wenn Sie als Trustee hinzugefügt wurden.

Abbildung 3-3 *Beispiel für ein globales Dashboard*



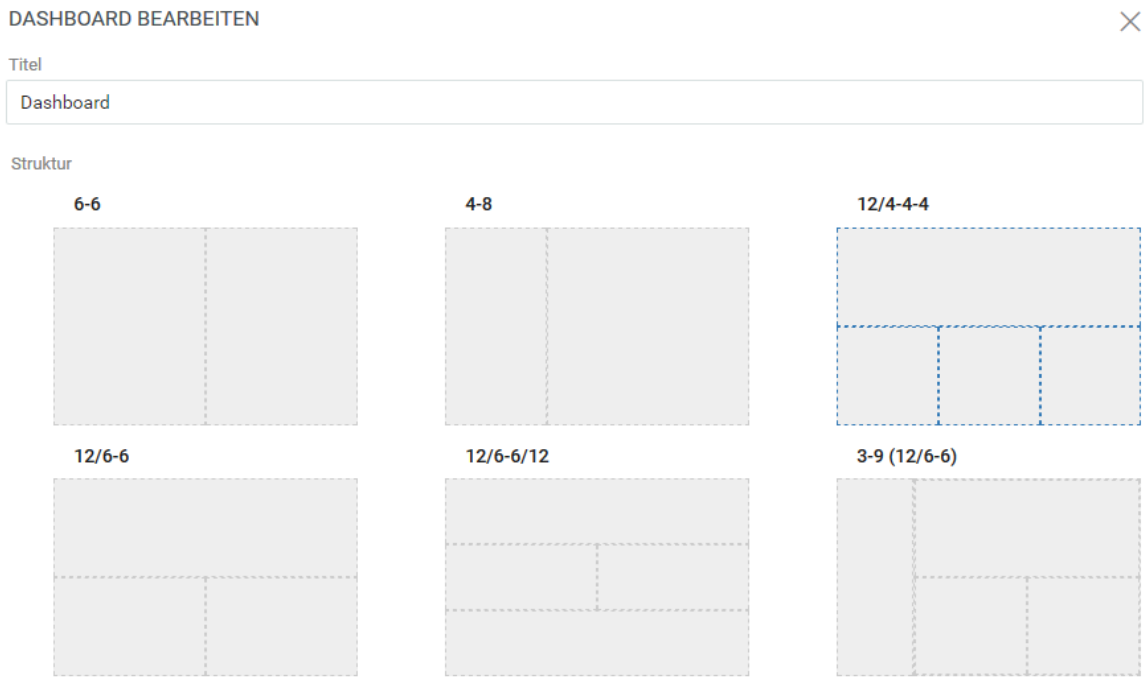
Der Administrator kann beliebige Benutzer, Container oder Rollen als Trustee zur Verwaltung des globalen Dashboards hinzufügen. Zum Bearbeiten der Trustees, die das Dashboard verwalten können, wählen Sie **Ihre ID > Einstellungen > Zugriff** und klicken Sie in der Liste auf **Globales Dashboard**. Weitere Informationen zum Bearbeiten des Konfigurationszugriffs finden Sie unter Managing Dashboard Widgets (Verwalten der Dashboard-Widgets) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

3.2 Ändern des Dashboard-Layouts

Die Identitätsanwendungen ermöglichen es Ihnen, das Layout des Erscheinungsbilds der Widgets am Dashboard zu bearbeiten.

1. Klicken Sie im **Dashboard** auf ∘∘∘.
2. Wählen Sie **Layout**.
3. Wählen Sie das Layout aus, das am Dashboard zu sehen sein soll.

Abbildung 3-4 *Ändern der Layouts*



WICHTIG: Klicken Sie zum Anwenden Ihrer Änderungen auf **Speichern**.

3.3 Hinzufügen eines Widgets

Wechseln Sie zum Hinzufügen neuer Widgets zum Dashboard zu **Dashboard**, klicken Sie auf ∘∘∘ und wählen Sie **Widgets** aus.

Abbildung 3-5 *Hinzufügen von Widgets*

3.3.1 Hinzufügen von allgemeinen Widgets

Mit der Kategorie **Allgemein** können Sie Ihrem Dashboard andere Widgets (neben den standardmäßigen Identity Manager-Widgets) hinzufügen. Geben Sie die REST API-URL des erforderlichen Widgets an und zeigen Sie die erforderlichen Informationen in Form von Linien-, Kreis- oder Tabellendiagrammen an.

1 Wählen Sie einen der folgenden Widget-Typen in der Liste aus:
   - **Liniendiagramm:** Zeigt die angeforderten Informationen für das ausgewählte Element in Form eines Liniendiagramms an.
   - **Verbindungen:** Gibt Ihnen die Möglichkeit, ein Lesezeichen für häufig verwendete Links anzulegen, mit denen Sie rasch auf diese Links zugreifen.
   - **Tortendiagramm:** Zeigt die angeforderten Informationen für das ausgewählte Element in Form eines Tortendiagramms an.
   - **Tabelle:** Listet die angeforderten Informationen für das ausgewählte Element in Tabellenform auf.

2 Mit ⚙ konfigurieren Sie das neue Widget im Dashboard.

3 (Bedingt) Geben Sie für die Widgets **Liniendiagramm**, **Tortendiagramm** und **Tabelle** die folgenden Details an:
   - **Titel:** Gibt den Namen des Widgets an, der am Dashboard angezeigt wird.
   - **URL:** Gibt die REST API-URL des erforderlichen Widgets an, das auf dem Dashboard angezeigt werden soll.
   - **Root-Element:** Gibt das Element des REST API-Codes an, für das ein Diagramm angezeigt werden soll. Groß-/Kleinschreibung wird in diesem Feld berücksichtigt. Sie müssen exakt den Namen angeben, der im REST API-Code angegeben ist.
   - **Spalten:** Gibt die Spalten an, die am Widget angezeigt werden sollen. Sie können mehrere Spalten hinzufügen. **Titel** gibt den Anzeigenamen für eine Spalte an. **Pfad** gibt den Spaltennamen an, der in der REST API genannt ist. Bei Eingabe im Feld **Pfad**ist auf die Groß- bzw. Kleinschreibung zu achten. Sie müssen exakt die Zeichenkette des REST API-Codes eingeben.

   Im folgenden Beispiel sehen Sie einen REST API-Code für die Seite **Rollen**:


```
{
    "total": 12,
    "nextIndex": 0,
    "token": "60045d6be10f4419a2da9fa728683b06",
    "assignments": [
        {
            "id":
"cn=aaacccc,cn=level30,cn=roledefs,cn=roleconfig,cn=appconfig,cn=user
application driver,cn=driverset1,o=system",
            "name": "AAAcccc",
            "description": "afasfdsf",
            "entityType": "role",
            "link": "/IDMProv/rest/access/assignments/item",
            "bulkRemovable": "true",
            "categories": [
                {
                    "categoryId": "default",
                    "categoryName": "Default"
                }
```

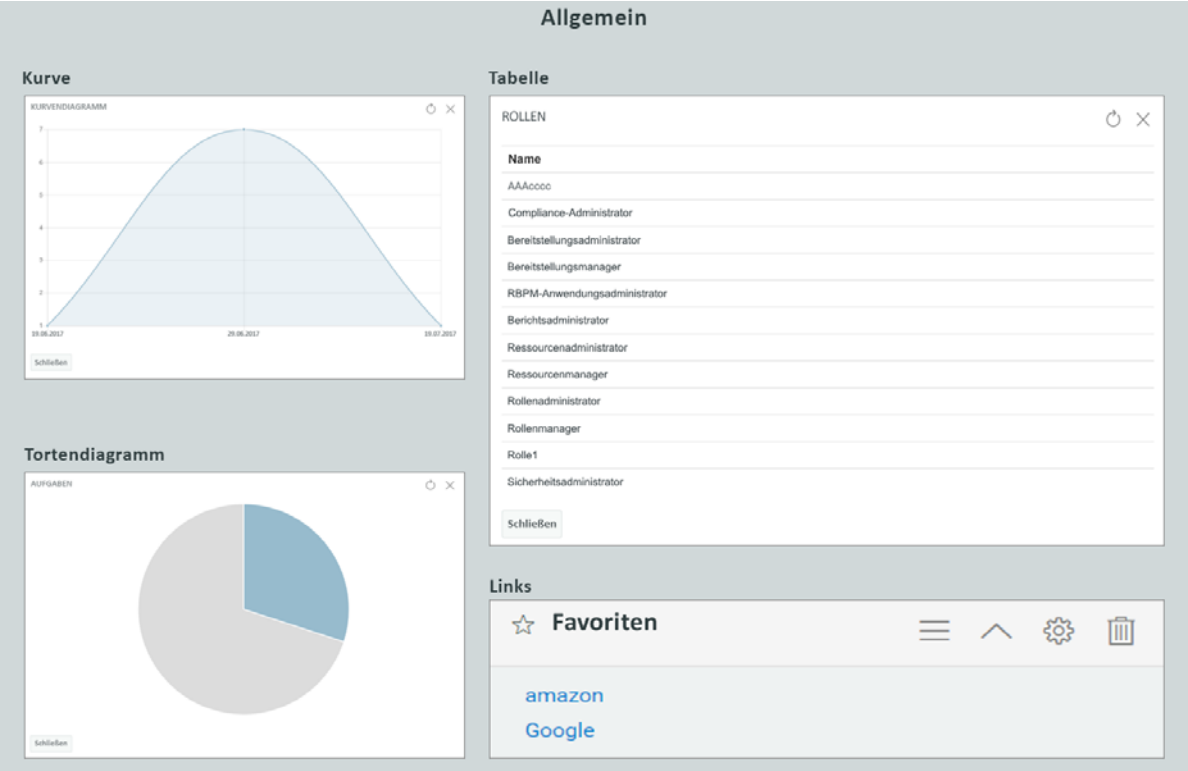
In diesem Beispiel bezeichnet "assignments" das Root-Element und "name" die ausgewählte Spalte, die am Widget angezeigt wird. Sie können auch ein Lesezeichen für jede beliebige URL setzen, auf die Sie vom Dashboard aus zugreifen möchten.

4 (Bedingt) Geben Sie bei Link-Widgets den **Titel** für die Links an und fügen Sie Links hinzu, auf die Sie vom Dashboard aus zugreifen möchten.

5 Klicken Sie zum Anwenden der Einstellungen auf **Speichern**.

Die folgenden Beispiele zeigen Diagramm- und Link-Widgets, die dem Dashboard hinzugefügt werden können:

Abbildung 3-6 *Beispiel für allgemeine Widgets*



3.3.2 Hinzufügen von Identity Manager-Widgets

Mit der Kategorie **IDM** können Sie Ihrem Dashboard standardmäßige Identity Manager-spezifische Widgets hinzufügen.

Beispiel:

- **Zugriff:** Zeigt die Anzahl der Rollen und Ressourcen sowie weitere Informationen dazu an.
- **Anforderungen für andere:** Zeigt ausstehende und abgelehnte Anforderungen für andere Benutzer an und gibt Ihnen die Möglichkeit, eine Anforderung für diese Benutzer zu erstellen.
- **Eigene Anforderungen:** Zeigt die Anzahl der ausstehenden und abgelehnten Anforderungen an und gibt Ihnen die Möglichkeit, eine neue Anforderung zu erstellen.
- **Aufgaben:** Zeigt die Anzahl der neuen oder ausstehenden Aufgaben oder die bald ablaufenden Aufgaben an.

Weitere Informationen zum Konfigurieren dieser Widgets finden Sie unter Abschnitt 3.4, „Konfigurieren von Widgets“, auf Seite 35.

WICHTIG: Klicken Sie zum Anwenden Ihrer Änderungen auf **Speichern**.

3.3.3 Hinzufügen von Identity Governance-Widgets

Sollen Identity Governance-Widgets verwendet werden, müssen Sie Identity Governance für das Identity Manager-Dashboard installieren und konfigurieren.

Mit der Kategorie „IG“ können Sie Ihrem Dashboard standardmäßige Identity Governance-spezifische Widgets hinzufügen. Beispiel:

Fulfillment-Aufgaben

Zeigt die Anzahl der Zugriffsanforderungen, Geschäftsrollen und Fehler im System.

Aufgaben prüfen

Zeigt die Anzahl der ausstehenden und erledigten Prüfungen im System.

Funktionstrennungsverletzungen

Zeigt die Anzahl der nicht geprüften, genehmigten oder behobenen Funktionstrennungsverletzungen im System.

3.3.4 Widget-Optionen

Für Widgets können Sie die folgenden Vorgänge ausführen:

Aktualisieren

Aktualisiert den Widget-Inhalt mit den aktuellen Informationen.

Repositionieren

Hiermit verschieben Sie das Widget an eine andere Stelle im Dashboard.

Konfigurieren

Hiermit konfigurieren Sie die Eigenschaften des Widgets. Weitere Informationen finden Sie unter Abschnitt 3.4, „Konfigurieren von Widgets“, auf Seite 35.

Entfernen

Löscht das Widget aus dem Dashboard.

Komprimieren

Blendet die Widget-Informationen aus und zeigt lediglich den Titel des Widgets an.

Widget als Vollbild öffnen

Zeigt die Widget-Informationen im Vollbildmodus an.

HINWEIS

- Die Optionen **Aktualisieren** und **Widget als Vollbild öffnen** werden nur für Widgets aus der Kategorie „Allgemein“ angezeigt.
- Klicken Sie zum Anwenden Ihrer Änderungen auf **Speichern**.

3.4 Konfigurieren von Widgets

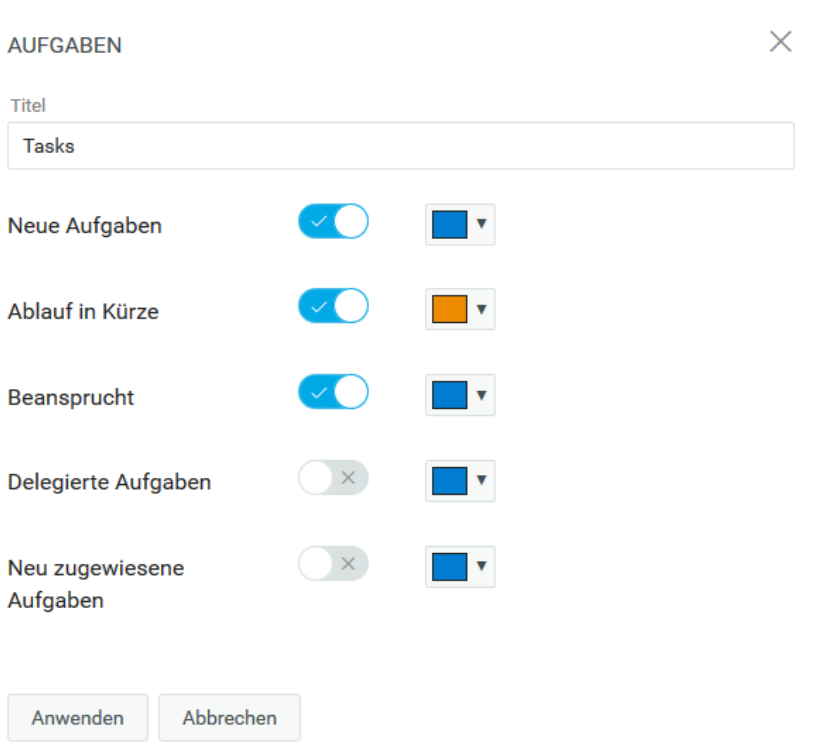
Jedes zum Dashboard hinzugefügte Widget kann konfiguriert werden. Sie können beispielsweise die Felder in einem Widget aktivieren oder deaktivieren oder auch die Anzeigefarbe der Felder ändern.

1. Klicken Sie auf ⚙ am Widget, das konfiguriert werden soll.
2. Bearbeiten Sie die Eigenschaften des Widgets.

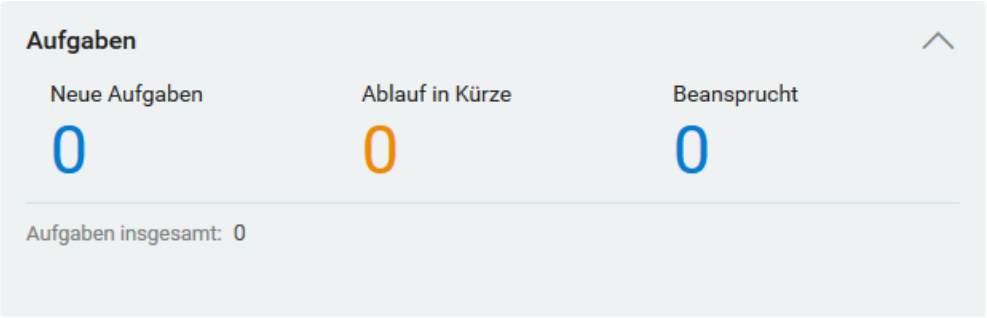
   Sie können beispielsweise den Titel eines Widgets ändern oder auch die Farbe der Beschriftung für ein Feld im Widget. Auf der Seite „Eigenschaften“ können Sie auch ein Widget-Feld aktivieren oder deaktivieren.
3. Klicken Sie auf **Anwenden**, um die Änderungen am Dashboard anzuzeigen.

Sie können beispielsweise das Widget „Aufgaben“ wie folgt bearbeiten:

Abbildung 3-7 *Beispiel für eine Widget-Konfiguration*



Klicken Sie auf **Anwenden**, um die Änderungen am Dashboard anzuzeigen.



Bearbeiten Sie zum Konfigurieren der allgemeinen Widgets die Optionen, die beim Hinzufügen von Widgets angezeigt werden. Siehe Abschnitt 3.3.1, „Hinzufügen von allgemeinen Widgets“, auf Seite 32.

WICHTIG: Klicken Sie zum Anwenden Ihrer Änderungen auf **Speichern**.

III Verwalten Ihrer Berechtigungen und Ihres Identitätsprofils

Über das Dashboard in NetIQ Identity Manager fordern Sie den Zugriff auf die Ressourcen und Rollen an, die Sie für Ihre tägliche Arbeit benötigen. In der Identity Manager-Umgebung können Sie außerdem alle Aufgaben bearbeiten, die Ihnen zugewiesen wurden, z. B. Zugriffsanforderungen genehmigen. Besitzer von Ressourcen und Rollen können den Prozess verwalten.

Wenn Sie eine Berechtigung anfordern, startet Identity Manager einen Prozess, mit dem Ihre Anforderung effizient geprüft wird, sodass Sie die benötigte Rolle oder Ressource erhalten können. Ihr Manager erhält entweder per Email oder im Dashboard eine Benachrichtigung, Ihre Anforderung zu prüfen. In bestimmten Fällen muss Ihre Anforderung auch von anderen Personen in Ihrer Organisation genehmigt werden.

Einige Benutzer können außerdem Anforderungen im Namen anderer Personen abgeben oder als Vertretung für einen anderen Benutzer auftreten.

4 Verwalten Ihrer Berechtigungsanforderungen

Dieser Abschnitt enthält Anweisungen für die folgenden Aufgaben:

Beachten Sie auch die Hilfeinformationen (?) zu diesen Aktivitäten im Dashboard.

4.1 Anzeigen Ihrer Berechtigungen

Zum Abrufen der Rollen und Ressourcen, auf die Sie zugreifen können, wählen Sie Folgendes im Dashboard:

Zugriff > Berechtigungen

Anschließend können Sie eine bestimmte Berechtigung auswählen und weitere Details zu dieser Rolle oder Ressource abrufen. In der Berechtigung werden ggf. auch die Gründe für die Zuweisung der Berechtigung angegeben. Zum Auffinden einer bestimmten Berechtigung in einer langen Liste können Sie nach dem Namen oder der Beschreibung der Berechtigung suchen. Außerdem können Sie die Liste filtern.

Ein Team-Manager oder Supervisor kann die Berechtigungen anderer Teammitglieder auf der Registerkarte **Sonstige** sehen.

HINWEIS: Standardmäßig wird die Liste der zugewiesenen oder genehmigten Berechtigungen angezeigt. Mit rufen Sie die untergeordneten Berechtigungen ab, die den zugewiesenen oder genehmigten Berechtigungen zugeordnet sind.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

4.2 Anfordern von Berechtigungen

Zum Anfordern von Rollen und Ressourcen wählen Sie Folgendes im Dashboard:

Zugriff > Anforderungen

Bevor Sie Berechtigungen anfordern, beachten Sie die folgenden Überlegungen:

- Eventuell können Sie den Zugriff im Namen eines anderen Benutzers anfordern. Als Team-Manager können Sie beispielsweise in der Regel im Namen der Teammitglieder handeln. Der Prozess ist nahezu identisch; Sie müssen lediglich angeben, dass die Anforderung für **Sonstige** Benutzer erfolgt statt für Sie **Selbst**.

- Geben Sie beim Anfordern einer Berechtigung keine Satzzeichen ein. Falls der Name der anzufordernden Berechtigung ein Satzzeichen enthält, lassen Sie die Satzzeichen bei der Suche weg.
- Für die unterschiedlichen Berechtigungen sind unterschiedliche Informationen erforderlich, abhängig davon, wie der Administrator das Berechtigungsformular konfiguriert hat. Wenn detaillierte Informationen für die Berechtigung erforderlich sind, werden Sie vom Dashboard an ein separates Fenster weitergeleitet, in dem Sie die Berechtigung auswählen.
- Sie können mehrere Berechtigungen gleichzeitig anfordern.

  Falls jedoch besondere Informationen im Berechtigungsformular für eine der Berechtigungen erforderlich sind, können Sie diese Berechtigung ggf. nicht in einer Anforderung nach mehreren Berechtigungen angeben. Sollen mehrere Berechtigungen gleichzeitig angefordert werden, dürfen keine detaillierten Informationen in den Anforderungsformularen für die verschiedenen Anforderungen erforderlich sein.
- Sie können das Ablaufdatum angeben, wenn Sie eine Ressource oder eine Rolle anfordern.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

4.3 Anzeigen von Anforderungen

Zum Abrufen des Status für eine laufende Anforderung und der erledigten Anforderungen wählen Sie Folgendes im Dashboard:

Zugriff > Anforderungsverlauf

Ein Team-Manager oder Supervisor kann den Anforderungsverlauf anderer Teammitglieder auf der Registerkarte **Sonstige** sehen.

Sie können auch ein Helpdesk-Ticket für Ihre ausstehenden Anforderungen erstellen.

- Abschnitt 4.3.1, „Verfolgen einer Anforderung“, auf Seite 40
- Abschnitt 4.3.2, „Abbrechen einer Anforderung“, auf Seite 41
- Abschnitt 4.3.3, „Erstellen eines Helpdesk-Tickets“, auf Seite 41

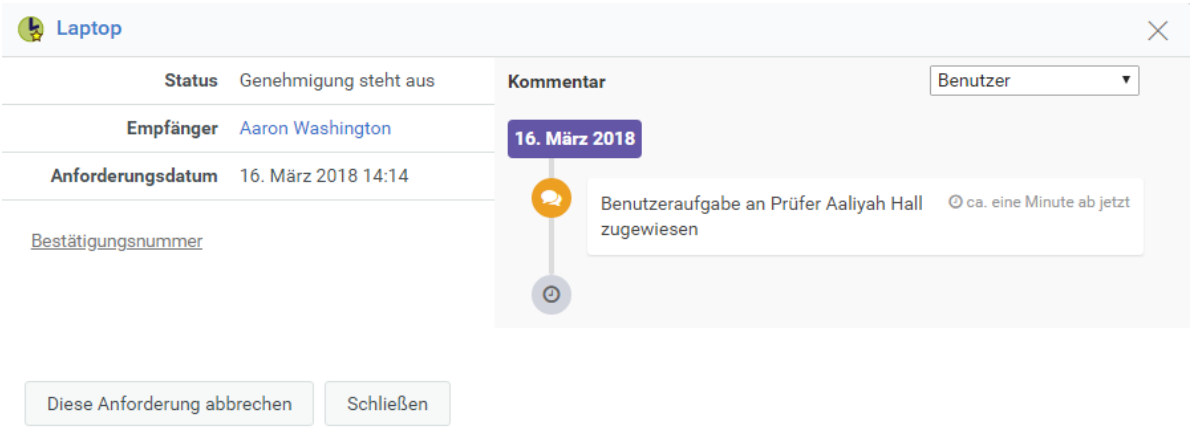
Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

4.3.1 Verfolgen einer Anforderung

Bei den einzelnen Anforderungen können Sie nicht nur Ihre Aktionen abrufen, sondern auch den Workflow zum Genehmigen oder Verweigern Ihrer Anforderung. Jeder Schritt im Prozess ist mit einem Zeitstempel versehen.

Zum Verfolgen einer ausstehenden Anforderung wählen Sie die Anforderung aus und klicken Sie oben rechts im Menü auf **Benutzer und System**. Im Dashboard wird der aktuelle Status der Anforderung im Genehmigungsprozess angezeigt.

Abbildung 4-1 *Verfolgen einer Anforderung*



4.3.2 Abbrechen einer Anforderung

Sie können eine *ausstehende* Anforderung über die Verlaufsliste abbrechen. Wählen Sie die Anforderung in der Liste aus und wählen Sie im nachfolgenden Fenster die Option **Diese Anforderung abbrechen**.

4.3.3 Erstellen eines Helpdesk-Tickets

Bei längeren Verzögerungen können Sie sich an den Helpdesk wenden.

An den folgenden Stellen können Sie ein Helpdesk-Ticket erstellen:

- **Zugriff > Anfordern**; klicken Sie auf **Helpdesk-Ticket**.
- **Anwendungen**; klicken Sie auf **Helpdesk-Ticket**.
- **Zugriff > Anforderungsverlauf**, klicken Sie auf in der Anforderung, für die ein Helpdesk-Ticket erstellt werden soll.

  Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

Die Helpdesk-Mitarbeiter werden über das Helpdesk-Ticket benachrichtigt. Sobald das Ticket behoben oder geschlossen wird, erhalten Sie eine Benachrichtigung.

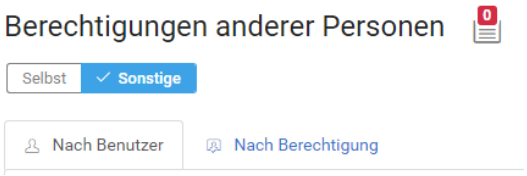
4.4 Entziehen von Berechtigungen

Wenn Sie keinen Zugriff mehr auf eine Rolle oder Ressource benötigen, können Sie die Berechtigung für diese Rolle oder Ressource wieder entziehen. Zum Entziehen einer Berechtigung navigieren Sie zu **Zugriff** > **Berechtigungen**, wählen die gewünschte Berechtigung aus und geben einen Grund für das Entziehen der Berechtigung an.

Sie können eine Berechtigung auch im Namen anderer Benutzer entziehen. Wenn Ihr Teammitglied beispielsweise aus Abteilung 1 zu Abteilung 2 gewechselt ist und keinen Zugriff mehr auf eine bestimmte Ressource benötigt, bietet Identity Manager eine Funktion, mit der Sie die Berechtigung für diesen Benutzer entziehen. Wählen Sie hierzu **Sonstige** und ziehen Sie die Berechtigung zurück. Sie können mehrere Berechtigungen gleichzeitig entziehen. Diese Berechtigungen können Sie zum Prüfen in eine Warteschlange stellen und dann später entziehen.

Nur der Administrator und ein Team-Manager können Berechtigungen für andere Benutzer entziehen. Ein Administrator kann Berechtigungen für alle Benutzer in der Organisation entziehen, ein Team-Manager dagegen nur für die jeweiligen Teammitglieder.

Zum Entziehen von Berechtigungen für andere Benutzer stehen folgende Verfahren zur Auswahl:



- **Nach Benutzer suchen:** Hiermit können Sie einen Benutzer suchen und die Berechtigungen für diesen Benutzer entziehen. Sie können eine Berechtigung für den Benutzer direkt entziehen oder diese Berechtigung in eine Warteschlange stellen. Eine Warteschlange ist ein permanenter Arbeitsbereich, in dem Berechtigungen vorübergehend gespeichert werden, sodass Sie sie prüfen und bei Bedarf entziehen können. Anschließend können Sie andere Berechtigungen suchen, die für diesen Benutzer entzogen werden sollen, und in die Warteschlange aufnehmen. So können Sie alle Berechtigungen gleichzeitig entziehen.
- **Nach Berechtigung suchen:** Hiermit können Sie eine bestimmte Berechtigung suchen. Wenn Sie eine Berechtigung auswählen, werden alle Benutzer aufgelistet, die diese Berechtigung besitzen. Sie können die Berechtigung für den ausgewählten Benutzer direkt entziehen oder diese Berechtigung in eine Warteschlange stellen und dann für mehrere Benutzer gleichzeitig entziehen.

Team-Manager: Als Team-Manager können Sie Ihrem Team die Berechtigungen auf der Registerkarte **Sonstige** entziehen. Sie können nur dann anderen Benutzern die Berechtigungen entziehen, wenn Sie die entsprechenden Berechtigungen besitzen.

Verwalter: Als Administrator können Sie einem Team-Manager die Entzugsberechtigung zuweisen. Dieser Fall tritt beispielsweise ein, wenn ein Team-Manager die Berechtigung „Rolle dem Benutzer entziehen“ erhalten soll. Wählen Sie **Personen > Teams** und bearbeiten Sie die Teamberechtigungen, sodass der Team-Manager die gewünschten Entzugsberechtigungen erhält.

Abbildung 4-2 *Beispiel zum Zuweisen einer Entzugsberechtigung für einen Team-Manager*

Mit dieser Option kann der Team-Manager den Teammitgliedern die ausgewählte Rolle entziehen.

HINWEIS: Wenn Sie eine Berechtigung entziehen, ist diese Änderung eventuell nicht sofort in der Berechtigungsliste sichtbar. Die Berechtigung ist mit einem Entzugsprozess verbunden, der eine gewisse Zeit in Anspruch nehmen kann. Aktualisieren Sie die Liste, damit die Änderungen angezeigt werden.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

5 Verwalten Ihrer Aufgaben

Wenn Sie für das Genehmigen und Verweigern angeforderter Berechtigungen in Identity Manager zuständig sind, verwalten Sie Ihre Aufgaben im Dashboard auf dieselbe Weise wie zuvor in der Benutzeranwendung. Sie können die Anforderungen einzeln genehmigen oder verweigern oder auch mehrere Anforderungen, für die keine detaillierten Informationen erforderlich sind, im Massenmodus genehmigen oder verweigern.

Zum Abrufen ausstehender Anforderungen wählen Sie Folgendes im Dashboard:

Aufgaben

Alternativ können Sie eine Email-Berechtigung mit einem Link erhalten, über den Sie eine Anforderung in einer Email-Antwort genehmigen oder verweigern.

Bevor Sie Benutzeranforderungen bearbeiten, beachten Sie die folgenden Überlegungen:

- Sie können mehrere Aufgaben zur Genehmigung/Verweigerung im Massenmodus auswählen.
- Bei einer komplexeren Anforderung, für die detaillierte Informationen erforderlich sind, wird im Dashboard kein Kontrollkästchen angezeigt. Zum Genehmigen oder Verweigern dieser Anforderungen müssen Sie die einzelnen Anforderungen auswählen und die Formulare ausfüllen.
- Wenn Sie eine komplexere Anforderung zur Genehmigung oder Verweigerung auswählen, wird das Anforderungsformular ggf. in einer separaten Registerkarte im Browser geöffnet.
- Im Allgemeinen müssen Sie einen Kommentar abgeben, in dem Sie erläutern, warum Sie die ausgewählten Aufgaben genehmigen oder verweigern.

5.1 Verwalten von Anforderungen zur Genehmigung oder Verweigerung

In einigen Organisationen ist möglicherweise eine Gruppe von Personen dafür zuständig, Zugriffsanforderungen zu überprüfen, zu genehmigen oder zu verweigern. In diesem Fall erhält jedes Mitglied der Gruppe dieselben Anforderungen. Beispiel: Das IT-Team ist verantwortlich für alle Anforderungen für Telekommunikationsgeräte und Computer. Wenn ein neuer Mitarbeiter ein Mobiltelefon anfordert, wird die Anforderung allen Mitgliedern des IT-Serviceteams zugewiesen. Jede Person im Team kann die Anforderung bearbeiten.

Sie können zur Anforderung eine der folgenden Aufgaben durchführen:

Anforderung beanspruchen

Sie können für eine Anforderung die **Zuständigkeit beanspruchen** und die erforderliche Aufgabe sofort oder später ausführen. Unabhängig davon, wann Sie entsprechend der Aufgabe agieren, sehen die Mitglieder Ihrer Gruppe diese Anforderung nicht mehr in ihren **Aufgaben**.

Anforderung freigeben

Wenn Sie die beanspruchte Anforderung nicht bearbeiten möchten, können Sie die Anforderung wieder freigeben.

Anforderung neu zuweisen

Eine Aufgabe, die Ihnen zugewiesen wurde, kann einem anderen Benutzer in der Organisation neu zugewiesen werden. Beim Neuzuweisen von Aufgaben sind die folgenden Punkte zu beachten:

- Wenn Sie die Aufgabe nicht erledigen können, haben Sie die Möglichkeit, sie Ihrem Manager neu zuzuweisen.
- Wenn Sie die Aufgabe nicht im angegebenen Zeitraum bearbeitet haben, können die folgenden Aktionen eintreten:
  - Ein Administrator kann die Aufgabe einem anderen Benutzer neu zuweisen. Ein Administrator besitzt eine Berechtigung, eine Aufgabe einem beliebigen Benutzer in der Organisation zuzuweisen.
  - Der Team-Manager kann die Aufgabe einem anderen Mitglied im Team zuweisen.
  - Der Helpdesk-Benutzer kann die Aufgabe Ihrem Manager zuweisen (bis zur Hierarchieebene, die auf der Seite **Einstellungen** definiert ist). Der Administrator konfiguriert die Managerhierarchie.

Wenn Ihnen eine Aufgabe neu zugewiesen wurde und Sie diese Aufgabe nicht übernehmen können, haben Sie die Möglichkeit, die Aufgabe an den Benutzer zurückzugeben, der sie Ihnen zugewiesen hat.

Anforderung zurückgeben

Wenn Sie eine Anforderung, die Ihnen neu zugewiesen wurde, nicht bearbeiten möchten, können Sie diese Anforderung zurückgeben. Die Identitätsanwendungen weisen die zurückgegebene Aufgabe automatisch wieder dem eigentlichen Genehmiger zu.

HINWEIS: Nur eine neu zugewiesene Anforderung kann zurückgegeben werden.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

5.2 Verwalten von Helpdesk-Aufgaben

Helpdesk-Aufgaben werden für jedes Helpdesk-Ticket generiert, das im System ausgelöst wurde. Im Beispiel in Abschnitt 1.6.4, „Wie funktioniert der Helpdesk?“, auf Seite 19 löst Emilys Ticket die Erstellung einer Helpdesk-Aufgabe auf Helens Seite **Aufgaben** aus. Helen kann entsprechende Maßnahmen für diese Helpdesk-Aufgabe ergreifen.

Als Helpdesk-Benutzer wählen Sie das Helpdesk-Ticket aus, das von Ihnen bearbeitet werden soll. Führen Sie eine der folgenden Aktionen für das ausgewählte Helpdesk-Ticket durch:

Aktualisierung

Aktualisiert das Helpdesk-Ticket mit einem geeigneten Kommentar.

Abgeschlossen

Schließt das Helpdesk-Ticket zusammen mit Ihrem Auflösungskommentar ab.

Abbrechen

Schließt das Helpdesk-Ticket mit einem geeigneten Kommentar.

HINWEIS: Sie können eine Helpdesk-Aufgabe **beanspruchen** oder **freigeben** Wenn Sie ein Helpdesk-Ticket in der Aufgabenliste beanspruchen, wird das Helpdesk-Ticket in Ihren **Selbst**-Aufgaben angezeigt.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

6 Handeln im Namen eines anderen Benutzers

In bestimmten Organisationen sind Sie ggf. berechtigt, Aufgaben als Vertretung oder Beauftragter für einen anderen Benutzer zu übernehmen. Ein/e persönliche/r Assistent/in kann beispielsweise Vertretungsaktionen für den/die Vorgesetzte/n ausführen. Auch wenn eine Kollegin im Mutterschutz ist, können Sie vorübergehend als ihre Vertretung ernannt werden.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

6.1 Anzeigen Ihrer Vertretungszuweisungen

Zum Abrufen Ihrer Vertretungszuweisungen wählen Sie Folgendes im Dashboard:

Zugriff > Vertretungszuweisungen

6.2 Vertreten anderer Benutzer

Ein Administrator kann Sie als Vertretung für einen anderen Benutzer zuweisen. In diesem Fall wird oben rechts in Ihrem Kontomenü eine Vertretungsoption eingetragen.

***Ihre ID* > Vertretung als**

Sarah Schmidt ist beispielsweise für Customer Relations zuständig. Die Identitätsanwendungen umfassen ein Customer-Relations-Team mit Sarah Schmidt als Team-Manager. Sie kann im Namen von Maria Belafonte auftreten, die Mitglied in ihrem Team ist. Im Dashboard wählt sie **ssschmidt > Vertretung als** und gibt dann **mbelafonte** an.

6.3 Verwaltung von Vertretungszuweisungen

Als Administrator oder Team-Manager können Sie eine Zuweisung erstellen, bearbeiten und löschen. Damit ein Team-Manager die Vertretungszuweisungen für ein Team verwalten kann, müssen Sie das Team entsprechend konfigurieren. Der Team-Manager kann Zuweisungen lediglich für Teammitglieder erstellen.

7 Verwalten von Delegierungen

In bestimmten Organisationen ist es möglich, Aufgaben an einen anderen Benutzer zu delegieren. Wenn Sie als Delegierter für die Aufgaben anderer Benutzer fungieren oder Ihre Aufgaben an andere Benutzer in der Organisation delegiert wurden, werden die Delegierungsinformationen unter **Administration > Delegierung** angezeigt.

Die delegierten Aufgaben werden auf der Seite **Aufgaben** aufgeführt.

HINWEIS: Die Aufgaben mit dem Symbol wurden delegiert.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

8 Verwalten Ihres Profils

Die Identitätsanwendungen bieten Ihnen eine komfortable Möglichkeit, Ihre Identitätsinformationen abzurufen und zu bearbeiten. Außerdem erhalten Sie hiermit bei Bedarf Zugriff auf Informationen zu anderen Benutzern, wodurch die Reaktionsfähigkeit Ihrer Organisation erhöht wird. Sie möchten beispielsweise:

- Ihr eigenes Benutzerkonto selbst verwalten
- Bei Bedarf nach Benutzern und Gruppen in der Organisation suchen
- Anzeigen, wie diese Benutzer und Gruppen in Zusammenhang stehen
- Anwendungen auflisten, mit denen Sie verknüpft sind

Ihr Systemadministrator ist für die Einrichtung des Inhalts der Identitätsanwendungen für Sie und andere Personen in Ihrer Organisation verantwortlich. Was Sie sehen und tun können, hängt in der Regel von Ihren Aufgaben und Ihrer hierarchischen Position in Ihrer Organisation ab.

8.1 Aktualisieren Ihres Profils

Zum Abrufen oder Aktualisieren Ihres Profils wählen Sie Folgendes im Dashboard aus:

***[Ihre ID]* > Mein Profil**

Oder,

Klicken Sie im Dashboard auf .

Auf dieser Seite werden Ihr Berichterstellungsmanager, Ihre Rollen und Ressourcen sowie Ihre Gruppe aufgelistet. Zum Bearbeiten Ihrer Informationen sowie zum Abrufen Ihres Organigramms benötigen Sie den Administratorzugriff.

Ihr Profil enthält Einstellungen wie Ihren Namen, Ihre Email-Adresse und Ihre Telefonnummer. Diese Seite zeigt die Benutzerattribute, die beim **Such**- und **Lese**-Zugriff aktiviert sind. Diese Zugriffseigenschaften können im Directory Abstraction Layer (DAL) konfiguriert werden. Weitere Informationen finden Sie unter Attributeigenschaften in *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications* (NetIQ Identity Manager – Administratorhandbuch zur Entwicklung der Identitätsanwendungen). Ihre Organisation legt fest, welche Einstellungen Sie bearbeiten können. Sie können beispielsweise Ihre Telefonnummer ändern, nicht jedoch Ihren Nachnamen.

9 Abrufen eines Organigramms

Das Dashboard umfasst ein Organigramm mit der Hierarchie der Benutzer in Ihrer Organisation.

Standardmäßig können der Sicherheitsadministrator und der Bereitstellungsadministrator das Organigramm für alle Benutzer im System abrufen. Mit den folgenden Verfahren navigieren Sie zum Organigramm:

- Wählen Sie **Personen > Organigramm**. Auf dieser Seite wird das Organigramm für den angemeldeten Benutzer angezeigt. Soll das Organigramm anderer Benutzer gesucht werden, die sich im System befinden, geben Sie den Namen dieser Benutzer in die Suchleiste ein.
- Wählen Sie **Personen > Benutzer**, wählen Sie einen Benutzer in der Liste aus und klicken Sie neben dem Benutzernamen auf das Symbol .

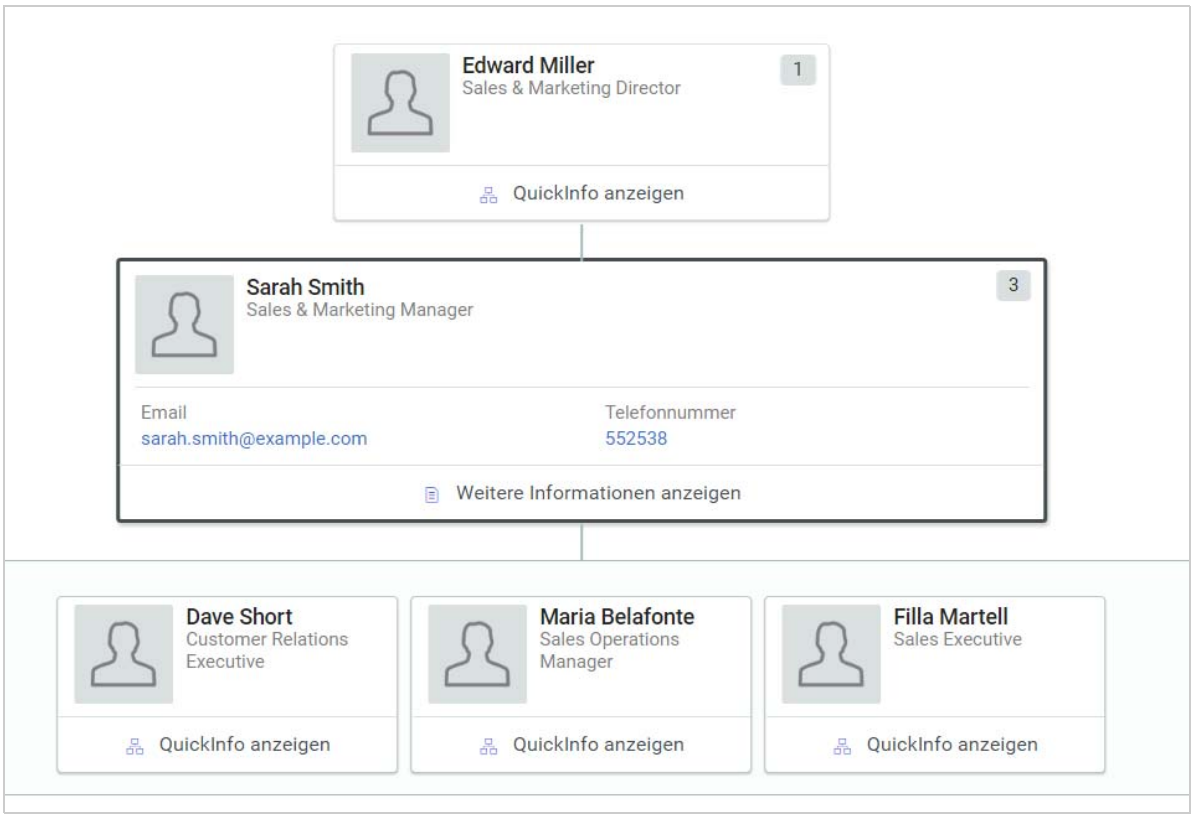
HINWEIS: Zum Abrufen des **Organigramms** benötigen Sie den **Organigramm**-Zugriff. Bitten Sie den Administrator, Ihnen diesen Zugriff zuzuweisen. Weitere Informationen finden Sie unter Managing User Access (Verwalten des Benutzerzugriffs) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

9.1 Grundlagen des Organigramms

Das Organigramm zeigt die Benutzerinformationen in Kartenform an, wobei die Karten in hierarchischer Reihenfolge angeordnet sind. Der Manager des ausgewählten Benutzers wird oben angezeigt, die direkt Unterstellten entsprechend unten.

Beispiel für ein Organigramm für die Benutzerin *Sarah Smith*:

Abbildung 9-1 *Beispiel für das Organigramm im Dashboard*



In diesem Beispiel fungiert *Edward Miller* als Manager von *Sarah Smith*; *Dave Short*, *Maria Belafonte* und *Filla Martell* sind *Sarah Smith* direkt unterstellt. Die Zahl oben rechts auf der Benutzerkarte bezeichnet die Anzahl der Personen, die diesem Benutzer direkt unterstellt sind.

Auf der ausgewählten Benutzerkarte sowie mit der Option **QuickInfo anzeigen** auf den anderen Benutzerkarten werden die grundlegenden Benutzerinformation angezeigt, die ein Administrator als Primärattribute festgelegt hat. Weitere Informationen zum Anpassen der Primärattribute finden Sie unter Customizing the Views (Anpassen der Ansichten) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

Mit **Weitere Informationen anzeigen** erhalten Sie weitere Informationen zum Benutzer in einer Benutzerliste.

10 Verwalten Ihres Passworts

Identity Manager bietet die Komponente Self Service Password Reset (SSPR), mit der Sie Passwörter ändern bzw. vergessene Passwörter zurücksetzen können. Falls das Passwort zurückgesetzt werden muss, greift SSPR zu Ihrer Authentifizierung auf diese Sicherheitsabfrage zurück.

HINWEIS: In diesem Abschnitt werden die Standardfunktionen der Passwortverwaltung beschrieben. Es ist möglich, dass Sie einige Unterschiede zwischen Ihrer Anwendung und den Beschreibungen in diesem Handbuch feststellen. Diese hängen mit Ihrer Rolle und Ihrer hierarchischen Position in der Organisation sowie mit möglichen organisationsbezogenen Anpassungen zusammen. Weitere Informationen erhalten Sie von Ihrem Systemadministrator.

10.1 Verwenden von Self-Service Password Management in Identity Manager

SSPR integriert sich automatisch in den von Identity Reporting und den Identitätsanwendungen verwendeten Single Sign-On-Prozess. Es ist das Standardprogramm von Identity Manager für die Passwortverwaltung. Wenn ein Benutzer eine Passwortzurücksetzung anfordert, fragt SSPR den Benutzer nach den Antworten auf seine persönliche Sicherheitsabfrage. Werden die Antworten korrekt eingegeben, reagiert SSPR auf eine der folgenden Weisen:

- Erlaubt dem Benutzer das Erstellen eines neuen Passworts
- Erstellt ein neues Passwort und sendet es dem Benutzer zu
- Erstellt ein neues Passwort, sendet es dem Benutzer zu und markiert das alte Passwort als abgelaufen

Die Reaktion von SSPR können Sie im SSPR-Konfigurationseditor festlegen. Nach einem Upgrade auf eine neue Version von Identity Manager können Sie SSPR so konfigurieren, dass Identity Manager weiterhin NMAS, die bisherige Methode der Passwortverwaltung, verwendet. Ihre bisherigen Passwortrichtlinien für die Verwaltung vergessener Passwörter erkennt SSPR allerdings nicht. Sie können SSPR auch so konfigurieren, dass es statt NMAS sein proprietäres Protokoll verwendet. Wenn Sie diese Änderung vornehmen, können Sie allerdings nicht mehr ohne Zurücksetzung Ihrer Passwortrichtlinien zu NMAS zurückkehren.

Mit SSPR können Sie mit jeder der in Tabelle 10-2 aufgeführten Funktionen arbeiten:

Tabelle 10-1 Funktionen zur Passwortverwaltung

Passwortverwaltungsseite	Aktion
Sicherheitsantwort für Passwort	Eine der beiden folgenden Optionen festlegen oder ändern: ◆ Ihre gültigen Antworten auf vom Administrator definierte Sicherheitsabfragen ◆ Benutzerdefinierte Sicherheitsabfragen und -antworten
Ändern des Passworts	Ihr Passwort gemäß den vom Systemadministrator festgelegten Regeln ändern (zurücksetzen)
Status der Passwortrichtlinie	Ihre Passwortrichtlinienanforderungen prüfen.

10.1.1 Grundlagen der Sicherheitsantwort für Passwort

Sicherheitsabfragen werden bei der Anmeldung zur Überprüfung Ihrer Identität verwendet, wenn Sie Ihr Passwort vergessen haben. Wenn der Systemadministrator eine Passwortrichtlinie für Sie eingerichtet hat, können Sie die Seite „Sicherheitsantwort für Passwort“ für folgende Aufgaben verwenden:

- Für Sie gültige Antworten auf vom Administrator definierte Fragen angeben
- Eigene Fragen und die zugehörigen Antworten festlegen (sofern Ihre Passwortrichtlinie dies ermöglicht)

In Identity Manager 4.5 werden Sie bei der Anmeldung automatisch auf die Seite mit der Sicherheitsabfrage weitergeleitet. Auf dieser Seite richten Sie die Antworten für die Sicherheitsfragen ein. Weitere Informationen finden Sie unter Abschnitt 2.4.1, „Vergessen des Passworts“, auf Seite 24. Wenn Sie sich erneut anmelden und versuchen, das vergessene Passwort zurückzusetzen, stellt Ihnen SSPR die hier konfigurierten Fragen und fordert Sie auf, die korrekten Antworten anzugeben. Stimmen Ihre Antworten mit den zuvor auf dieser Seite gespeicherten Eingaben überein, können Sie Ihr Passwort zurücksetzen.

10.1.2 Ändern Ihres Passworts

Sie können Ihr Passwort ändern (sofern der Systemadministrator diese Funktion für Sie aktiviert hat).

1. Klicken Sie im Dashboard auf **Anwendungen > Passwort ändern**.
2. Geben Sie Ihr aktuelles Passwort ein. Die Seite „Passwort ändern“ wird angezeigt.

3. Geben Sie das neue Passwort in das Textfeld **Neues Passwort** ein.

4 Geben Sie das neue Passwort erneut in das Textfeld **Passwort bestätigen** ein.

5 Klicken Sie auf **Passwort ändern**.

Wenn Ihr neues Passwort die von Ihrem Administrator in der Passwortrichtlinie definierten Passwortregeln verletzt, sehen Sie eine Fehlermeldung auf der Seite "Passwort ändern".

Auf dieser Seite ist in der Regel auch angegeben, wie ein Passwort aussehen muss, um die Anforderungen der vom Administrator festgelegten Richtlinien zu erfüllen. Lesen Sie die Passwortregeln und versuchen Sie es danach erneut mit einem entsprechenden Passwort.

6 Klicken Sie auf **Fortfahren**. Der Status Ihrer Anforderung wird angezeigt. Bei Erfolg werden Sie zur OSP-Anmeldeseite zurückgeleitet.

10.1.3 Status der Passwortrichtlinie

HINWEIS: Diese Funktion steht nur verwaltungsbefugten Benutzern zur Verfügung.

Ihr Administrator weist Ihnen einen Passwortrichtlinie zu. Diese Richtlinie legt die Ihrem Passwort zugrunde liegenden Sicherheitsbedingungen fest. Die Bedingungen Ihrer Passwortrichtlinie können Sie nur einsehen, wenn Ihnen der Administrator der Benutzeranwendung das Recht hierfür erteilt hat. Der Administrator der Benutzeranwendung hat hingegen auf der Startseite von Identity Manager die Möglichkeit, den Status Ihrer Passwortrichtlinie zu kontrollieren. Dieser Link ist jedoch nicht standardmäßig vorhanden. Um ihn anzuzeigen, müssen Sie die Startseite anpassen. Informationen zur Anpassung der Startseite von Identity Manager finden Sie im Abschnitt „Configuring Identity Manager Home “ (Konfigurieren der Startseitenelemente von Einrichtungshandbuch zu NetIQ Identity Manager) im *Benutzerhandbuch zu NetIQ Identity Manager-Startseite und Bereitstellungs-Dashboard*.

Klicken Sie auf der Landingpage auf den Link **Passwortstatus und -richtlinie**. Die Seite **Passwortstatus und -richtlinie** wird angezeigt. Wenn Sie Ihr Passwort für Identity Manager ändern möchten, gehen Sie zur Startseite von Identity Manager und wählen Sie Passwort ändern aus. Über den Startseiten-Link von Identity Manager werden Sie in den Passwortänderungsbereich von SSPR weitergeleitet.

10.2 Verwenden der bisherigen Passwortverwaltung

In diesem Abschnitt wird erläutert, wie Sie die Seiten der Passwortverwaltung auf der Registerkarte **Identitätsselbstbedienung** der Identity Manager-Benutzeranwendung verwenden. Es werden u. a. folgende Themen erläutert:

HINWEIS: In diesem Abschnitt werden die Standardfunktionen der Seiten zur Passwortverwaltung beschrieben. Es ist möglich, dass Sie einige Unterschiede zwischen Ihrer Anwendung und den Beschreibungen in diesem Handbuch feststellen. Diese hängen mit Ihrer Rolle und Ihrer hierarchischen Position in der Organisation sowie mit möglichen organisationsbezogenen Anpassungen zusammen. Weitere Informationen erhalten Sie von Ihrem Systemadministrator.

Allgemeine Informationen zum Aufrufen und Arbeiten mit der Registerkarte **Identitätsselbstbedienung** finden Sie in Kapitel 8, „Verwalten Ihres Profils“, auf Seite 51.

Auf den Seiten zur Passwortverwaltung können Sie alle in Tabelle 10-2 aufgeführten Funktionen durchführen:

Tabelle 10-2 *Funktionen zur Passwortverwaltung*

Passwortverwaltungsseite	Aktion
Sicherheitsantwort für Passwort	Eine der beiden folgenden Optionen festlegen oder ändern: ◆ Ihre gültigen Antworten auf vom Administrator definierte Sicherheitsabfragen ◆ Benutzerdefinierte Sicherheitsabfragen und -antworten
Änderung des Passworthinweises	Ihren Passworthinweis festlegen oder ändern
Änderung des Passworts	Ihr Passwort gemäß den vom Systemadministrator festgelegten Regeln ändern (zurücksetzen)
Status der Passwortrichtlinie	Ihre Passwortrichtlinienanforderungen prüfen.
Passwortsynchronisierungsstatus	Den Status der Synchronisierung von Anwendungspasswörtern mit dem Identitätsdepot anzeigen **HINWEIS:** Der Zugriff auf Anwendungen, die noch nicht vollständig synchronisiert wurden, kann zu Zugriffsproblemen führen.

10.2.1 Sicherheitsantwort für Passwort

Sicherheitsabfragen werden bei der Anmeldung zur Überprüfung Ihrer Identität verwendet, wenn Sie Ihr Passwort vergessen haben. Wenn der Systemadministrator eine Passwortrichtlinie für Sie eingerichtet hat, können Sie die Seite „Sicherheitsantwort für Passwort“ für folgende Aufgaben verwenden:

- Für Sie gültige Antworten auf vom Administrator definierte Fragen angeben
- Eigene Fragen und die zugehörigen Antworten festlegen (sofern Ihre Passwortrichtlinie dies ermöglicht)

So verwenden Sie die Seite „Sicherheitsantwort für Passwort“:

1. Klicken Sie auf der Registerkarte **Identitätsselbstbedienung** im Menü auf **Sicherheitsantwort für Passwort** (unter **Passwortverwaltung**).

   Die Seite „Sicherheitsantwort für Passwort“ wird angezeigt.
2. Geben Sie in jedes **Antwort**-Textfeld eine Antwort ein (es sind alle erforderlich) oder verwenden Sie die zuvor gespeicherten Antworten. Wenn die Option **Gespeicherte Antwort verwenden** ausgewählt ist, werden die Sicherheitsantworten einschließlich der Bezeichnungen nicht angezeigt. Darüber hinaus sind benutzerdefinierte Sicherheitsfragen deaktiviert.

   Stellen Sie sicher, dass Sie Antworten angeben, an die Sie sich später erinnern können.
3. Geben Sie alle erforderlichen benutzerdefinierten Fragen an oder ändern Sie sie. Es ist nicht möglich, eine Frage mehrfach zu verwenden.

4 Klicken Sie auf **Senden**.

Nachdem Sie die Sicherheitsantworten gespeichert haben, zeigt die Benutzeranwendung eine Meldung an, die angibt, dass die Sicherheitsantworten erfolgreich gespeichert wurden, und es wird erneut der Bildschirm für die Sicherheitsantworten angezeigt, in dem die Option „Gespeicherte Antwort verwenden?“ ausgewählt ist.

10.2.2 Änderung des Passworthinweises

Ein Passworthinweis wird bei der Anmeldung verwendet und soll Ihnen helfen, sich an Ihr Passwort zu erinnern, wenn Sie dieses vergessen haben. Auf der Seite „Änderung des Passworthinweises“ können Sie Ihren Passworthinweis festlegen oder ändern.

1 Klicken Sie auf der Registerkarte **Identitätsselbstbedienung** im Menü auf **Änderung des Passworthinweises** (unter **Passwortverwaltung**).

Die Seite „Passworthinweisdefinition“ wird angezeigt.

2 Geben Sie den neuen Hinweistext ein.

Ihr Passwort darf nicht im Hinweistext enthalten sein.

3 Klicken Sie auf **Senden**.

Der Status Ihrer Anforderung wird angezeigt.

10.2.3 Änderung des Passworts

Auf dieser Seite können Sie jederzeit Ihr Passwort ändern, sofern der Systemadministrator Ihnen die hierfür erforderliche Berechtigung erteilt hat.

1 Klicken Sie auf der Registerkarte **Identitätsselbstbedienung** im Menü auf **Passwort ändern** (unter **Passwortverwaltung**).

Die Seite „Passwort ändern“ wird angezeigt. Wenn Ihr Systemadministrator eine entsprechende Passwortrichtlinie für Sie eingerichtet hat, wird auf der Seite „Passwort ändern“ in der Regel angegeben, wie ein Passwort zu definieren ist, damit es den Anforderungen der Richtlinie entspricht. Beispiel:

Wenn keine Passwortrichtlinie eingerichtet wurde, wird einfach die standardmäßige Seite „Passwort ändern“ mit Feldern zum Ändern Ihres Passworts angezeigt.

Ab Version 4.0.2 unterstützt die Benutzeranwendung die folgenden Passwortsyntaxtypen:

- Microsoft-Komplexitätsrichtlinie

  Dieser Passwortsyntaxtyp wird für die Rückwärtskompatibilität mit Active Directory 2003 verwendet.

- Passwortrichtlinie von Microsoft Server 2008

  Dies ist ein neuer Passwortsyntaxtyp, der zu eDirectory 8.8.7 hinzugefügt wurde, um Active Directory 2008 zu unterstützen.

  Die folgenden Einstellungen werden von der Microsoft Server 2008-Passwortrichtlinie unterstützt:

  - Verwendung der Passwortrichtlinie von Microsoft Server 2008
  - Maximale Anzahl der Komplexitätsrichtlinienverletzungen im Passwort (0–5)

- Novell-Syntax

Die folgenden neuen Einstellungen werden von der Novell-Syntax unterstützt:

- Mindestanzahl von nicht alphabetischen Zeichen (1–512)
- Maximale Anzahl von nicht alphabetischen Zeichen (1–512)

Für alle drei Passwortsyntaxtypen unterstützt die Benutzeranwendung die folgenden Funktionen:

- Anzahl der Zeichen, die vom aktuellen Passwort und von den früheren Passwörtern abweichen (0–6)
- Anzahl der früheren Passwörter, die für den Ausschluss von Zeichen berücksichtigt werden sollen (0–10)

Wenn Ihr Administrator die Syntax der Microsoft Server 2008-Richtlinie aktiviert hat, müssen Sie auf der Seite „Passwort ändern“ folgende Felder ausfüllen:

2 Geben Sie Ihr aktuelles Passwort in das Textfeld **Altes Passwort** ein.

3 Geben Sie das neue Passwort in das Textfeld **Neues Passwort** ein.

4 Geben Sie das neue Passwort erneut in das Textfeld **Passwort wiederholen** ein.

5 Klicken Sie auf **Senden**.

Wenn Ihr neues Passwort die von Ihrem Administrator definierten Passwortregeln verletzt, sehen Sie eine Fehlermeldung auf der Seite „Passwort ändern“. Wenn Sie die Microsoft Server 2008-Richtlinie verwenden und Ihr Passwort sie verletzt, wird auf der Benutzeroberfläche diese Meldung oben auf der Seite angezeigt:

```
Password AD2008 complexity policy violation.
```

Wenn Ihr neues Passwort die Regeln verletzt, sehen Sie sich die von Ihrem Administrator definierten Passwortregeln an und versuchen Sie es erneut.

6 Möglicherweise werden Sie aufgefordert, einen Passworthinweis einzugeben, wenn der Administrator Ihre Sicherheitsrichtlinie so konfiguriert hat. Lesen Sie in diesem Fall den Abschnitt 10.2.2, „Änderung des Passworthinweises“, auf Seite 59.

7 Der Status Ihrer Anforderung wird angezeigt.

10.2.4 Status der Passwortrichtlinie

Ihr Administrator weist Ihnen einen Passwortrichtlinie zu. Diese Richtlinie legt die Ihrem Passwort zugrunde liegenden Sicherheitsbedingungen fest. Sie können die Anforderungen Ihrer Passwortrichtlinie wie folgt überprüfen:

1 Klicken Sie auf der Registerkarte **Identitätsselbstbedienung** im Menü auf **Status der Passwortrichtlinie** (unter **Passwortverwaltung**). Die Seite **Status der Passwortrichtlinie** wird angezeigt.

Elemente, die als „ungültig“ markiert sind, können nicht geändert werden.

10.2.5 Passwortsynchronisierungsstatus

Auf der Seite „Passwortsynchronisierungsstatus“ können Sie überprüfen, ob Ihr Passwort mit anderen Anwendungen synchronisiert wurde. Verwenden Sie eine andere Anwendung nur nach erfolgter Synchronisierung Ihres Passworts. Der Zugriff auf Anwendungen, die noch nicht vollständig synchronisiert wurden, kann zu Zugriffsproblemen führen.

1 Klicken Sie auf der Registerkarte **Identitätsselbstbedienung** im Menü auf **Passwortsynchronisierungsstatus** (unter **Passwortverwaltung**). Die Seite **Passwortsynchronisierungsstatus** wird angezeigt. Vollfarbige Symbole zeigen Anwendungen an, mit denen das Passwort synchronisiert wurde. Grau dargestellte Symbole zeigen Anwendungen an, die noch nicht synchronisiert wurden.

HINWEIS: Das Feld **Benutzer wählen** wird nur dem Administrator angezeigt.

IV Verwalten von Benutzern, Gruppen und Teams

Wenn Sie die entsprechende Rolle in den Identitätsanwendungen besitzen, können Sie Benutzer, Gruppen und Teams erstellen und verwalten. Sie können Benutzer und Teams im Dashboard und in der Benutzeranwendung erstellen. Gruppen werden in der Benutzeranwendung erstellt und verwaltet.

Systemadministratoren können Benutzer und Gruppen erstellen. Der Systemadministrator kann anderen Personen (in der Regel ausgewählten Mitarbeitern in Verwaltungs- oder Managementpositionen) Zugriff auf diese Funktion erteilen.

Möglicherweise unterscheiden sich einige der hier beschriebenen Funktionen von den Funktionen in Ihrer Anwendung. Dies hängt mit Ihrer Rolle und Ihrer hierarchischen Position in der Organisation sowie mit möglichen organisationsbezogenen Anpassungen zusammen. Weitere Informationen erhalten Sie von Ihrem Systemadministrator.

Auf der Seite „Verzeichnissuche“ können Sie prüfen, welche Benutzer oder Gruppen bereits vorhanden sind. Weitere Informationen hierzu finden Sie in Anhang B, „Verwenden der Verzeichnissuche in der Benutzeranwendung“, auf Seite 85.

Ein Team stellt eine Anzahl von Benutzern oder Gruppen oder von Benutzern und Gruppen dar, die dem Team zugeordnete Bereitstellungsanforderungen und Genehmigungsaufgaben durchführen können. Obwohl ein Team möglicherweise mit einer Gruppe übereinstimmt, die im Benutzerverzeichnis vorhanden ist, sind Teams nicht dasselbe wie Gruppen. Eine Gruppe oder ein Mitglied einer Gruppe kann keine Teamfunktionen ausführen, es sei denn, sie sind einem Team zugewiesen. Siehe Kapitel 12, „Verwalten von Teams“, auf Seite 71.

11 Verwalten von Benutzern)

In diesem Abschnitt wird erläutert, wie Sie Benutzer und Gruppen im Dashboard und in der Benutzeranwendung erstellen. Es werden u. a. folgende Themen erläutert:

11.1 Erstellen von Benutzern

Die Seite **Benutzer erstellen** zeigt die Benutzerattribute, die beim **Such**- und **Lese**-Zugriff aktiviert sind. Diese Zugriffseigenschaften können im Directory Abstraction Layer (DAL) konfiguriert werden. Weitere Informationen finden Sie unter Attributeigenschaften in *NetIQ Identity Manager - Administrator’s Guide to Designing the Identity Applications* NetIQ Identity Manager – Administratorhandbuch zur Entwicklung der Identitätsanwendungen.

Zum Erstellen eines Benutzers wählen Sie Folgendes im Dashboard:

Personen > Benutzer > +

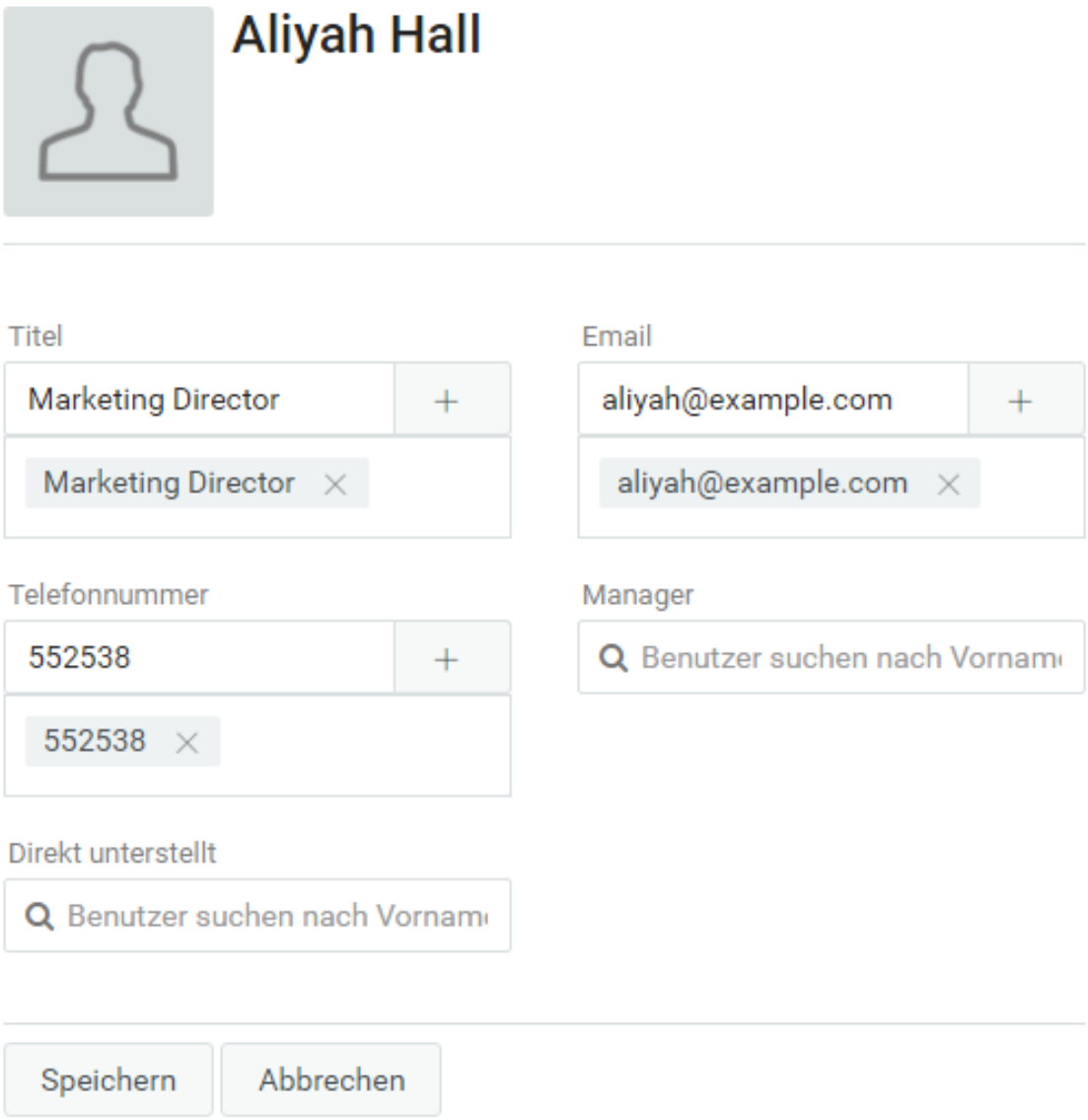
Der Identitätsadministrator definiert die Werte, die Sie für den Benutzer angeben können. Beim Erstellen eines Benutzers sehen Sie außerdem den **Benutzercontainer**, doch Sie können dessen Wert nicht ändern. Diese Einschränkung sorgt dafür, dass alle Benutzer in demselben Container gespeichert werden.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

11.2 Bearbeiten der Benutzerinformationen

Wählen Sie einen Benutzer in einer Listenansicht aus und klicken Sie auf ☑. Nun können Sie die Benutzerinformationen bearbeiten, z. B. Titel, Email-Adresse, Telefonnummer, Manager und vieles mehr. Beispiel für die Bearbeitung von Benutzerinformationen:

Abbildung 11-1 *Bearbeiten der Benutzerinformationen*



Sie können die Benutzerattribute bearbeiten, die der Administrator festgelegt hat. Weitere Informationen zum Konfigurieren der Benutzerattribute finden Sie unter Customizing the Views (Anpassen der Ansichten) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

In der Ansicht **Benutzer verwalten** können Sie Benutzer löschen.

11.3 Auflisten von Benutzern

Zum Auflisten der Benutzer in den Identitätsanwendungen stehen die folgenden Verfahren zur Auswahl:

- **Listenansicht:** Mit werden die Benutzer in Listenform dargestellt. Die Benutzerinformationen werden dabei auf der rechten Seite angezeigt. Zum Bearbeiten der Benutzerinformationen wie Telefonnummer, Email, Manager etc. klicken Sie auf . Mit rufen Sie das Organigramm für einen bestimmten Benutzer ab.
- **Kartenansicht:** Mit werden die Benutzer in Kartenform dargestellt. Damit werden die grundlegenden Informationen der Benutzer auf Karten angezeigt. Der Administrator kann die Informationen konfigurieren, die auf der Karte der einzelnen Benutzer angezeigt werden sollen. Weitere Informationen finden Sie unter Customizing the Views (Anpassen der Ansichten) im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*. Mit bearbeiten Sie die Benutzerinformationen, z. B. **Telefonnummer**, **Email**, **Manager** und andere Attribute. Mit rufen Sie das Organigramm für einen bestimmten Benutzer ab.
- **Ansicht „Benutzer verwalten“:** Mit werden die Benutzer in Tabellenform dargestellt. Damit werden die Benutzer in Tabellenform angezeigt. In dieser Ansicht können Sie die Benutzer nach den Benutzerattributen sortieren, z. B. Telefonnummer, Email, Abteilung und vieles mehr. Sie können die Spalten festlegen, die in dieser Ansicht angezeigt werden sollen. Weitere Informationen zum Anpassen von Spalten finden Sie in der Hilfe () im Dashboard.

  In dieser Ansicht können Sie auch Benutzer aus dem System löschen. So löschen Sie Benutzer:

  1. Wählen Sie einen zu löschenden Benutzer aus.
  2. Klicken Sie auf .

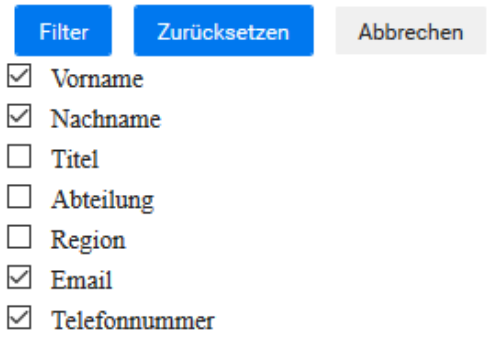
11.4 Suchen nach Benutzern

Zum Suchen nach Benutzern in den Identitätsanwendungen stehen die folgenden Verfahren zur Auswahl:

- **Schnellsuche:** Gibt das Benutzerattribut an und listet die Benutzer anhand der ausgewählten Filter auf. So bearbeiten Sie die Filteroptionen:

  1. Klicken Sie auf .
  2. Wählen Sie die Filteroptionen zum Suchen nach Benutzern.

     Das folgende Beispiel zeigt die ausgewählten Benutzerattribute für eine Schnellsuche:



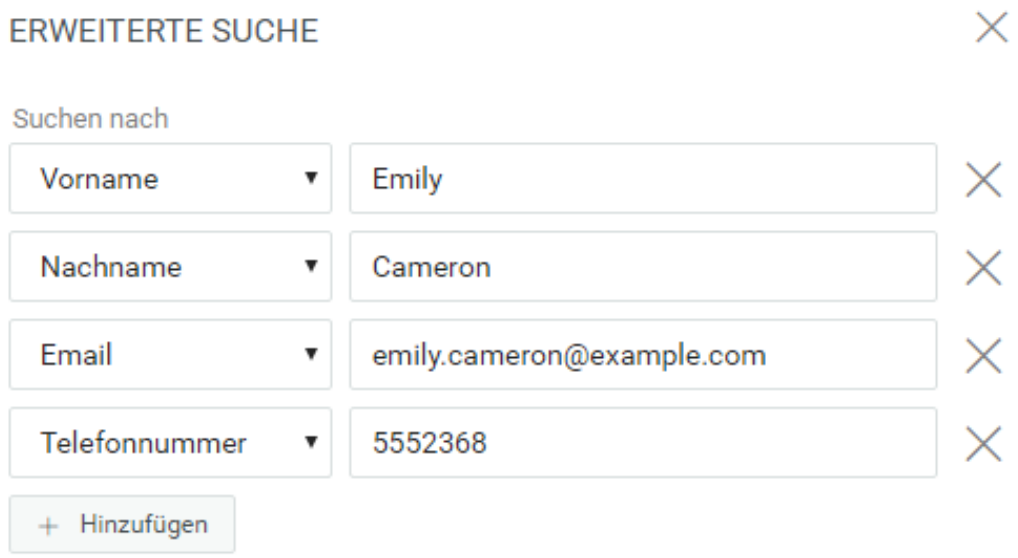
  3. Klicken Sie auf **Filter**.

Beispiel: Sie suchen einen Benutzer mit dem Namen Schmidt und wählen die Filter „Vorname“ und „Nachname“ aus. Die Schnellsuche gibt alle Benutzer zurück, deren Vorname oder Nachname den Namen Schmidt enthält.

- **Erweiterte Suche:** Diese Option gibt eine stärker verfeinerte Liste mit Benutzern zurück als die Schnellsuche. Sie können einen Benutzer anhand der definierten Benutzerattribute suchen. So verwenden Sie die erweiterte Suche:

  1. Klicken Sie auf ⊕.
  2. Geben Sie die genauen Benutzerinformationen für die einzelnen Benutzerattribute an.

     Das folgende Beispiel zeigt die angegebenen Benutzerattribute für eine erweiterte Suche:



  3. Klicken Sie auf **Filter**.

  Beispiel: Sie suchen einen Benutzer mit dem **Vornamen** Aliyah, dem **Nachnamen** Hall und dem **Titel** Direktor. Sie können diese Attribute in der erweiterten Suche festlegen und damit einen Benutzer suchen, der genau diese Attribute aufweist.

Darüber hinaus können Sie die Suchergebnisse auf einer Seite anhand des Index am unteren Rand konfigurieren. Das Dashboard arbeitet mit der VLV-Steuerung (Virtual List View), die an der LDAP-OID 2.16.840.1.113730.3.4 ausgeführt wird. Diese Steuerung kommt in Kombination mit der Sortiersteuerung zum Einsatz.

Das Identity Manager-Dashboard zeigt zwei verschiedene Anzahlen in den Ergebnissen:

- **Gesamtanzahl:** Gesamtanzahl aller Benutzer im System.
- **Suchanzahl:** Anzahl der Benutzer für die spezielle Suche.

11.5 Sortieren von Benutzern

In der Ansicht „Benutzer verwalten“ können Sie die Benutzer nach ihren Attributen sortieren. Der Administrator muss zusammengesetzte Indizes für die Benutzerattribute konfigurieren, damit die Benutzer sortiert werden können. Weitere Informationen zum Erstellen von Verbundindizes finden Sie unter Erstellen von Verbundindizes im *Einrichtungshandbuch zu NetIQ Identity Manager für Windows*.

HINWEIS: Falls Sie die Benutzer nicht nach den Benutzerattributen sortieren können, bitten Sie Ihren Administrator, einen zusammengesetzten Index für das gewünschte Attribut zu konfigurieren.

12 Verwalten von Teams

Ein Team besteht aus zwei Benutzertypen, beispielsweise:

Anforderer

Führt Berechtigungsanforderungen im Namen von anderen Teammitgliedern (den Empfängern) durch. Abhängig davon, wie das Team konfiguriert ist, kann ein Anforderer entsprechend einer einzelnen Bereitstellungsanforderung, einer oder mehrerer Anforderungskategorien oder aller Anforderungen agieren.

Der Anforderer verwaltet auch die Vertretungszuweisungen für Teammitglieder.

Empfänger

Mitglied des Teams, in dessen Namen Anforderer agieren können.

Teamempfänger können Benutzer oder Gruppen im Verzeichnis sein. Sie können auch direkt aus Verzeichnisbeziehungen stammen. Beispielsweise lässt sich eine Mitgliedsliste aus der Manager-Mitarbeiter-Beziehung in der Organisation ableiten. In diesem Fall wären die Teammitglieder all die Benutzer, die dem Team-Manager unterstellt sind.

HINWEIS: Der Bereitstellungsadministrator kann die Verzeichnisabstraktionsschicht so konfigurieren, dass kaskadierende Beziehungen unterstützt werden. In diesem Fall können mehrere Ebenen innerhalb einer Organisation in einem Team enthalten sein. Die Anzahl der Ebenen wird vom Administrator konfiguriert.

Zum Ausführen der folgenden Tätigkeiten wählen Sie jeweils **Personen > Teams**:

- Abschnitt 12.1, „Teams anzeigen“, auf Seite 71
- Abschnitt 12.2, „Erstellen eines Teams“, auf Seite 72
- Abschnitt 12.3, „Team bearbeiten“, auf Seite 72

12.1 Teams anzeigen

Auf der Seite **Teams** sind alle Teams aufgelistet, zu deren Anzeige Sie berechtigt sind. Sie sind möglicherweise Mitglied bei allen aufgelisteten Teams. Außerdem sind Sie vielleicht auch ein Administrator mit Berechtigungen zum Anzeigen, Bearbeiten oder Löschen bestimmter Teams, auch wenn Sie kein Mitglied sind.

Als Teammitglied sind Sie möglicherweise ein **Anforderer** und können Anforderungen im Namen anderer Teammitglieder vornehmen. Andere Personen im Team können möglicherweise auch diese Aktionen für Sie, den **Empfänger** ausführen. Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

12.2 Erstellen eines Teams

Als Administrator können Sie Teams erstellen. Ein **Team** stellt eine Anzahl von Benutzern oder Gruppen oder von Benutzern und Gruppen dar, die dem Team zugeordnete Bereitstellungsanforderungen und Genehmigungsaufgaben durchführen können.

Für jedes Team geben Sie die Teammitglieder (**Empfänger**) an, die die Berechtigungen des Teams erhalten sowie die Teammitglieder, die im Namen der Empfänger agieren dürfen (**Anforderer**). Nach dem Erstellen eines Teams können Sie die **Berechtigungen** (Ressourcen und Bereitstellungsanforderungsdefinitionen) angeben, die für die Teammitglieder gelten. Beispielsweise können Sie eine Notebook-Ressource hinzufügen, die Teammitglieder möglicherweise benötigen.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

12.3 Team bearbeiten

Als Administrator können Sie Teams bearbeiten und löschen. Sie können die folgenden Aspekte eines Teams bearbeiten:

- Name und Beschreibung des Teams ändern
- Anforderer für das Team bearbeiten.
- Teammitglieder hinzufügen oder entfernen.
- Berechtigungen für einen Team-Manager hinzufügen oder entfernen.

Weitere Informationen finden Sie in der Hilfe (?) im Dashboard.

13 Erstellen von Gruppen

Wenn Sie eine Administratorrolle in den Identitätsanwendungen besitzen, können Sie eine Gruppe erstellen.

1 Melden Sie sich bei der Benutzeranwendung an.

2 Klicken Sie auf der Registerkarte **Identitätsselbstbedienung** im Menü auf **Benutzer oder Gruppe erstellen** (unter **Verzeichnisverwaltung**, sofern angezeigt).

   Das Fenster **Zu erstellendes Objekt auswählen** wird angezeigt.

3 Wählen Sie in der Dropdown-Liste **Objekttyp** den Eintrag **Gruppe** aus und klicken Sie auf **Weiter**.

   Das Fenster **Gruppe - Attribute festlegen** wird angezeigt.

4 Geben Sie Werte für die folgenden erforderlichen Attribute an:

Attribut	Anzugebender Wert
Gruppen-ID	Der Name dieser neuen Gruppe.
Container	Eine organisatorische Einheit (OU) im Identitätsdepot, unter der Sie die neue Gruppe speichern möchten (z. B. die OU „Gruppen“). Beispiel: `ou=groups,ou=MyUnit,o=MyOrg` Informationen zur Verwendung der Schaltflächen, die für die Angabe eines Containers zur Verfügung stehen, finden Sie in Abschnitt 11.1, „Erstellen von Benutzern“, auf Seite 65. **HINWEIS:** Sie werden nicht zur Angabe eines **Containers** aufgefordert, wenn der Systemadministrator einen Standardcontainer für diesen Objekttyp eingerichtet hat.
Beschreibung	Eine Beschreibung der neuen Gruppe.

5 Klicken Sie auf **Weiter**.

   Die Gruppe wird erstellt. Anschließend wird das Fenster **Überprüfen** angezeigt.

   Das Fenster **Überprüfen** enthält optionale Links, die möglicherweise nützlich für Sie sind:

   - Klicken Sie auf den Namen der neuen Gruppe, um die zugehörige Profilseite mit detaillierten Informationen anzuzeigen.

     Auf der Profilseite können Sie die Daten der Gruppe bearbeiten oder die Gruppe löschen.

   - Klicken Sie auf **Weiteres Objekt erstellen**, um zum ersten Fenster der Seite „Benutzer oder Gruppe erstellen“ zurückzukehren.

V Anhang

Der folgende Anhang bietet zusätzliche Referenzinformationen und weiterführende Themen zur Identity Manager-Benutzeranwendung.

A Verwenden der Identity Manager Approvals App

Neben der von Identity Manager-Benutzern verwendeten Benutzeranwendung gibt es nun auch eine neue iOS-App, mit der Identity Manager-Benutzer Anforderungen über das rollenbasierte Bereitstellungsmodul von Identity Manager remote genehmigen oder ablehnen können.

Nach der Installation und Konfiguration der Approvals App stehen Ihnen in dieser App die gleichen Genehmigungsaufgaben zur Verfügung wie an der Benutzeranwendungsschnittstelle. Alle Änderungen werden zwischen der Approvals App und der Benutzeranwendung synchronisiert.

Sollten Sie vom Server des rollenbasierten Bereitstellungsmoduls von Identity Manager getrennt sein, können Sie auch im Offline-Modus arbeiten. Die Approvals App synchronisiert dann alle Änderungen automatisch, sobald die Verbindung wieder hergestellt ist.

In diesem Anhang erhalten Sie Informationen zur Installation und Verwendung der neuen Approvals App. Informationen für Identity Manager-Administratoren, die ihre Umgebung so konfigurieren müssen, dass ihre Benutzer die App verwenden können, finden Sie im Abschnitt „Konfigurieren der Identity Manager Approvals App“ im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

Ausführliche Informationen zur Approvals App finden Sie in den folgenden Abschnitten:

A.1 Anforderungen an das Produkt

Die Approvals App kann nur auf einem Apple iPhone oder iPad mit Apple iOS 5, iOS 6 oder iOS 7 installiert werden.

HINWEIS: Wenn Ihr Administrator die Verwendung der Approvals App noch nicht aktiviert hat, lässt sich die App nach der Installation vermutlich nicht konfigurieren. Informationen für Identity Manager-Administratoren, die die Identity Manager-Umgebung für die Verwendung der App konfigurieren müssen, finden Sie im Abschnitt „Konfigurieren der Identity Manager Approvals App“ im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

A.2 Installieren der Approvals App

Die NetIQ Identity Manager Approvals App können Sie von der Seite Approvals App (http://appstore.com/NetIQIdentityManagerApprovals) im Apple App Store auf Ihrem Gerät installieren.

Nach der Installation der Approvals App müssen Sie die App so konfigurieren, dass sie eine Verbindung zum Server des rollenbasierten Bereitstellungsmoduls von Identity Manager herstellen kann.

HINWEIS: Falls Ihr Passwort für die Benutzeranwendung abgelaufen ist, empfehlen wir Ihnen eine Änderung Ihres Passworts vor der Installation und Konfiguration der Approvals App. Denn falls die Passwortrichtlinie Ihrer Umgebung nach dem Ablauf eines Passworts nur eine begrenzte Anzahl an Kulanzanmeldungen zulässt, kann es passieren, dass die Approvals App bei dem Versuch, Ihre Identity Manager-Aufgaben mit dem Gerät zu synchronisieren, alle diese Kulanzanmeldungen aufbraucht.

A.3 Konfigurieren der Approvals App

Die NetIQ Identity Manager Approvals App kann je nach Anforderungen in Ihrer Umgebung und der Art der Konfiguration von Identity Manager auf verschiedene Weisen konfiguriert werden:

- Sie können in der Benutzeranwendung eine Anforderung für den Zugriff auf die Approvals App stellen und die App dann über den von Ihrem Identity Manager-Administrator bereitgestellten Email-Link auf Ihrem Gerät starten. Über diesen Link erhalten Sie auch alle erforderlichen Konfigurationsinformationen.
- Sie können auf Ihrem Gerät auf einen Konfigurationslink klicken oder einen Konfigurations-QR-Code einscannen, wobei Sie über diesen Link bzw. den QR-Code entweder alle erforderlichen Konfigurationsinformationen oder allgemeine Konfigurationsinformationen für Ihr Unternehmen erhalten.
- Sie können die Konfigurationsinformationen für Ihre Umgebung manuell in der App eingeben.

WICHTIG: Die Approvals App kann nur dann automatisch über einen Link oder einen QR-Code konfiguriert werden, wenn der Administrator der Identity Manager-Umgebung den Link oder QR-Code aktiviert hat.

A.3.1 Anfordern des Mobilzugriffs über die Benutzeranwendung

Wenn von Ihrem Administrator entsprechend konfiguriert, können Sie den Zugriff auf die Approvals App über die Benutzeranwendung anfordern. Identity Manager sendet daraufhin eine Email mit einem angepassten Link, den Sie auf Ihrem Gerät lediglich öffnen müssen, um die App automatisch mit Ihren Informationen zu konfigurieren.

So fordern Sie Mobilzugriff über die Benutzeranwendung an:

1. Melden Sie sich in einem Webbrowser mit dem HTTPS-Protokoll (`https://`) bei der Identity Manager-Benutzeranwendung an.

   HINWEIS: Zur Anforderung des Zugriffs auf die Approvals App müssen Sie über das HTTPS-Protokoll bei der Benutzeranwendung angemeldet sein.

   ---

2. Klicken Sie auf **Prozessanforderung senden**.

3 Klicken Sie auf das Dropdown-Menü „Prozessanforderungskategorie“ und wählen Sie **Konten** aus.

4 Klicken Sie auf **Fortfahren**.

5 Klicken Sie auf **Mobile Genehmigungsanwendung anfordern**.

HINWEIS: Die Prozessanforderungskategorie und der Name können, je nachdem, wie Ihr Administrator den Anforderungsprozess für die Approvals App konfiguriert hat, abweichen.

---

6 Geben Sie die erforderlichen Informationen in das Prozessanforderungsformular ein und klicken Sie auf **Senden**.

7 Sobald Sie nun eine Email Ihres Identity Manager-Administrators erhalten, öffnen Sie diese auf Ihrem Gerät und klicken Sie auf den darin enthaltenen Link, um eine Verbindung zwischen dem Gerät und dem Server des rollenbasierten Bereitstellungsmoduls herzustellen.

HINWEIS: Falls Sie die App bereits installiert haben, wird eventuell eine Warnung angezeigt, die Sie darauf hinweist, dass vorhandene Einstellungen überschrieben werden. Stellen Sie sicher, dass der in der Warnung angegebene Hostname identisch mit dem Namen des Hosts ist, auf den Sie bei der Anforderung des Zugriffs auf die App zugegriffen haben. Klicken Sie im Zweifelsfall nicht auf den Link, sondern kontaktieren Sie Ihren Administrator.

Wenn der Hostname korrekt ist, klicken Sie auf **Akzeptieren**, um die vorhandenen Einstellungen zu überschreiben.

---

8 Geben Sie nach dem Start der App Ihr Passwort ein und klicken Sie auf das Symbol „Verbindung testen“  , um Ihre Einstellungen zu überprüfen.

A.3.2 Verwenden eines Konfigurationslinks oder QR-Codes

Möglicherweise hat Ihr Identity Manager-Administrator für die Konfiguration Ihrer Approvals App einen Konfigurationslink bereitgestellt. Wenn Sie diesen Link in einem Browser auf Ihrem Gerät öffnen, wird die App automatisch konfiguriert.

Allerdings kann dieser Link nur einen Teil der erforderlichen Einstellungen bereitstellen. In der Regel stellt ein solcher Link oder Code nur die Details für den Server des rollenbasierten Bereitstellungsmoduls bereit, die zum Funktionieren der Approvals App absolut erforderlich sind. Nachdem Sie auf diesen Link geklickt haben, müssen Sie Ihren `Benutzernamen` und Ihr `Passwort` wie auch alle anderen nicht automatisch konfigurierten Einstellungen noch manuell eingeben.

In manchen Umgebungen haben Sie über Ihr Gerät keinen Zugriff auf Ihre Emails. Wenn Sie über Ihr Gerät keine Emails empfangen, können Sie sich stattdessen von Ihrem Identity Manager-Administrator einen personalisierten QR-Code geben lassen und diesen auf dem Gerät einscannen.

Zeigen Sie den personalisierten QR-Code dazu auf Ihrem Computer an oder drucken Sie ihn aus und scannen Sie ihn mit einem QR-Code-Leser auf Ihrem Gerät ein. Nachdem Sie die Approvals App mit dem QR-Code automatisch für Ihre Umgebung konfiguriert haben, geben Sie noch manuell Ihren `Benutzernamen` und Ihr `Passwort` ein.

A.3.3 Manuelles Konfigurieren der Approvals App

Falls der Administrator Ihrer Identity Manager-Umgebung keinen Link oder QR-Code für die Konfiguration der Approvals App bereitgestellt hat, können Sie die erforderlichen Einstellungen auch manuell konfigurieren.

WARNUNG: Da für die manuelle Konfiguration der App auf einem Mobilgerät genaue Kenntnisse der Identity Manager-Komponenten erforderlich sind, empfehlen wir nur erfahrenen Benutzern, die mit dem rollenbasierten Bereitstellungsmodul und der in Ihrem Unternehmen eingerichteten Benutzeranwendungsumgebung absolut vertraut sind, eine manuelle Konfiguration der App-Einstellungen. Allen anderen Benutzern legen wir nahe, sich zur Konfiguration der App an ihren Identity Manager-Administrator zu wenden.

Klicken Sie zur Konfiguration in der App auf das Symbol „Einstellungen“ , konfigurieren Sie die erforderlichen Einstellungen und klicken Sie dann auf das Symbol „Verbindung testen“ , um Ihre Einstellungen zu überprüfen.

Für die Approvals App sind folgende Einstellungen erforderlich:

Name der Anmeldeeinstellung	Beschreibung der Anmeldeeinstellung
Username (Benutzername)	Gibt Ihren Benutzernamen für den Zugriff auf den Server des rollenbasierten Bereitstellungsmoduls an.
Password (Passwort)	Gibt Ihr Passwort für den Zugriff auf den Server des rollenbasierten Bereitstellungsmoduls an.
Data Sync (Datensynchronisierung)	Gibt an, ob die App die Datensynchronisierung mit dem Server des rollenbasierten Bereitstellungsmoduls aktiv betreiben soll.
Advanced > Server Details > Server (Erweitert > Serverdetails > Server)	Gibt den vollständig qualifizierten Domänennamen oder die IP-Adresse des Servers des rollenbasierten Bereitstellungsmoduls an.
Advanced > Server Details > Secure Port (Erweitert > Serverdetails > Sicherer Port)	Gibt den HTTPS-Port an, über den die App die Verbindung mit dem Server herstellt.
Advanced > Server Details > Context (Erweitert > Serverdetails > Kontext)	Gibt den Kontext an, der bei der Installation der WAR-Datei der Benutzeranwendung verwendet wurde. Der Standardwert lautet `IDMProv`.
Advanced > Server Details > User Container (Erweitert > Serverdetails > Benutzercontainer)	Gibt den vollständigen eindeutigen Namen (DN) des Identitätsdepotcontainers an, in dem Benutzerinformationen gespeichert werden.
Advanced > Server Details > Timeout (Erweitert > Serverdetails > Zeitüberschreitung)	Gibt an, wie lange (in Sekunden) die App bei einem Verbindungsversuch mit dem Server wartet, bis sie den Versuch abbricht. Der Standardwert ist 5.
Advanced > Data Definition Settings > User Entity (Erweitert > Datendefinitionseinstellungen > Benutzerentität)	Gibt die LDAP-Entität an, die einen Benutzer im Identitätsdepot darstellt. Der Standardwert lautet `user`.
Advanced > Data Definition Settings > Name Format (Erweitert > Datendefinitionseinstellungen > Namensformat)	Gibt die DAL-Attributsdarstellung an, die die App zur Formatierung des vollständigen Namens eines Benutzers verwendet. Der Standardwert lautet `FirstName LastName`.
Advanced > Data Definition Settings > First Name Attr (Erweitert > Datendefinitionseinstellungen > Vornamensattribut)	Gibt den Namen des DAL-Attributs an, das den Vornamen eines Benutzers darstellt. Der Standardwert lautet `FirstName`.

Name der Anmeldeeinstellung	Beschreibung der Anmeldeeinstellung
Advanced > Data Definition Settings > Last Name Attr (Erweitert > Datendefinitionseinstellungen > Nachnamensattribut)	Gibt den Namen des DAL-Attributs an, das den Nachnamen eines Benutzers darstellt. Der Standardwert lautet `LastName`.
Advanced > Data Definition Settings > User Photo Attr (Erweitert > Datendefinitionseinstellungen > Benutzerfotoattribut)	Gibt den Namen des DAL-Attributs an, das das Foto eines Benutzers enthält. Der Standardwert lautet `UserPhoto`. **HINWEIS:** Wenn Sie in Identity Manager kein Foto konfiguriert haben bzw. Identity Manager so konfiguriert haben, dass kein Foto angezeigt wird, zeigt die App ein generisches Bild an.
Advanced > Data Definition Settings > Work Phone Attr (Erweitert > Datendefinitionseinstellungen > Geschäftstelefonattribut)	Gibt den Namen des DAL-Attributs an, das die geschäftliche Telefonnummer eines Benutzers darstellt. Der Standardwert lautet `TelephoneNumber`.
Advanced > Data Definition Settings > Mobile Phone Attr (Erweitert > Datendefinitionseinstellungen > Mobiltelefonattribut)	Gibt den Namen des DAL-Attributs an, das die Mobiltelefonnummer eines Benutzers darstellt. Der Standardwert lautet `mobile`.
Advanced > Data Definition Settings > Email Attr (Erweitert > Datendefinitionseinstellungen > Email-Attribut)	Gibt den Namen des DAL-Attributs an, das die Email-Adresse eines Benutzers darstellt. Der Standardwert lautet `Email`.
Advanced > Data Definition Settings > Photo LDAP Attr (Erweitert > Datendefinitionseinstellungen > Foto-LDAP-Attribut)	Gibt den Namen des DAL-Attributs an, das das Foto eines Benutzers enthält. Der Standardwert lautet `photo`.
Advanced > Data Definition Settings > Naming Attribute (Erweitert > Datendefinitionseinstellungen > Benennungsattribut)	Gibt das DAL-Benennungsattribut an, das im Identitätsdepot zur Beschreibung eines Namens verwendet wird. Der Standardwert lautet `cn`.
Advanced > Data Definition Settings > Provisioning Admin (Erweitert > Datendefinitionseinstellungen > Bereitstellungsadministrator)	Gibt an, ob Sie auf dem Server des rollenbasierten Bereitstellungsmoduls als Bereitstellungsadministrator geführt werden.
Advanced > Accepted Certificates (Erweitert > Akzeptierte Zertifikate)	Gibt alle ungültigen oder selbst signierten Zertifikate des Servers des rollenbasierten Bereitstellungsmoduls an, die die Approvals App akzeptieren soll. Wenn die Approvals App ein ungültiges oder selbstsigniertes Zertifikat erkennt, werden Sie gefragt, ob das Zertifikat akzeptiert oder abgelehnt werden soll. Wenn Sie ein solches Zertifikat akzeptieren, fügt es die App zur Liste der akzeptierten Zertifikate hinzu. Zertifikate aus dieser Liste können Sie entfernen, indem Sie auf den Namen des Zertifikats klicken und die App neu starten. **HINWEIS:** Ist ein Zertifikat des Servers des rollenbasierten Bereitstellungsmoduls ohnehin gültig, wird es nicht zur Liste der akzeptierten Zertifikate hinzugefügt. Gültige Zertifikate werden standardmäßig akzeptiert.

Name der Anmeldeeinstellung	Beschreibung der Anmeldeeinstellung
Advanced > Rejected Certificates (Erweitert > Abgelehnte Zertifikate)	Gibt alle ungültigen oder selbstsignierten Zertifikate des Servers des rollenbasierten Bereitstellungsmoduls an, die die Approvals App ablehnen soll. Wenn die Approvals App ein ungültiges oder selbstsigniertes Zertifikat erkennt, werden Sie gefragt, ob das Zertifikat akzeptiert oder abgelehnt werden soll. Wenn Sie ein solches Zertifikat ablehnen, fügt es die App zur Liste der abgelehnten Zertifikate hinzu. Legt der Server ein abgelehntes Zertifikat vor, kann die App keine Verbindung mit dem Server herstellen. Zertifikate aus dieser Liste können Sie entfernen, indem Sie auf den Namen des Zertifikats klicken.

A.4 Übersicht über die Approvals App

Dieser Abschnitt gibt eine Übersicht über die Benutzeroberfläche der NetIQ Identity Manager Approvals App. Es werden u. a. folgende Themen erläutert:

- Abschnitt A.4.1, „Aufgabenansicht“, auf Seite 82
- Abschnitt A.4.2, „Detailansicht“, auf Seite 82
- Abschnitt A.4.3, „Massenmodus“, auf Seite 83
- Abschnitt A.4.4, „Ansicht mit abgeschlossenen Aufgaben“, auf Seite 83
- Abschnitt A.4.5, „Ansicht mit Anmeldeeinstellungen“, auf Seite 83
- Abschnitt A.4.6, „Ansicht mit erweiterten Einstellungen“, auf Seite 84

A.4.1 Aufgabenansicht

Die Standardansicht der Approvals App ist die Aufgabenansicht. In dieser Ansicht werden alle Aufgaben angezeigt, die Ihnen zurzeit zugewiesen sind bzw. die Sie beansprucht haben. Angezeigt werden der Aufgabentitel und Name und das Bild des Aufgabenempfängers. Die Aufgaben sind in dieser Ansicht nach Ablaufdatum sortiert. Aufgaben mit dem frühesten Fälligkeitsdatum werden ganz oben und Aufgaben ohne Ablaufdatum ganz unten angezeigt.

HINWEIS: Wenn ein Benutzer in Identity Manager kein Foto konfiguriert hat bzw. er Identity Manager so konfiguriert hat, dass kein Foto angezeigt wird, zeigt die App ein generisches Bild an.

Wenn Sie eine Anforderung genehmigen oder ablehnen möchten oder die Details einer bestimmten Aufgabe anzeigen möchten, klicken Sie auf die Aufgabe bzw. auf den Namen des Aufgabenempfängers. Wenn Sie einen Aufgabenempfänger kontaktieren möchten, klicken Sie auf dessen Bild.

A.4.2 Detailansicht

In dieser Ansicht werden die Details einer bestimmten, Ihnen zugewiesenen Aufgabe angezeigt. Je nach Anforderung werden unterschiedliche Felder angezeigt.

Zum Genehmigen oder Ablehnen einer Aufgabe geben Sie die erforderlichen Informationen ein und klicken Sie auf **Genehmigen** bzw. **Ablehnen**.

A.4.3 Massenmodus

Falls Sie sehr viele ähnliche Aufgaben genehmigen oder ablehnen müssen, können Sie in der Aufgabenansicht von dem standardmäßigen Einzelaufgabenmodus in den Massenmodus wechseln.

HINWEIS: Nicht alle Aufgaben können jedoch im Massenmodus genehmigt werden. Komplexere Aufgaben, zum Beispiel Beglaubigungen, müssen Sie im Einzelaufgabenmodus genehmigen. Sobald Sie auf das Symbol für den Massenmodus geklickt haben, werden in der Aufgabenliste nur noch diejenigen Aufgaben angezeigt, die in diesem Modus genehmigt werden können.

So genehmigen bzw. lehnen Sie mehrere Aufgaben ab:

1. Klicken Sie in der Aufgabenansicht auf das Symbol für den Massenmodus .
2. Wählen Sie die Aufgaben aus, die Sie genehmigen oder ablehnen möchten. Es ist nicht möglich, gleichzeitig einige Aufgaben zu genehmigen und andere abzulehnen.
3. (Optional) Wenn Sie alle Aufgaben genehmigen oder ablehnen möchten, klicken Sie auf **Alle**.
4. (Optional) Falls Sie Ihre Meinung ändern und doch keine Aufgaben genehmigen oder ablehnen möchten, klicken Sie auf das Symbol für den Einzelaufgabenmodus .
5. Klicken Sie auf **Genehmigen** oder **Ablehnen**.
6. (Optional) Fügen Sie einen Kommentar zu diesem Massenvorgang hinzu.
7. Klicken Sie auf **Bestätigen**.

A.4.4 Ansicht mit abgeschlossenen Aufgaben

Wenn Sie nur Ihre bereits abgeschlossenen Aufgaben anzeigen möchten, klicken Sie auf das Symbol für abgeschlossene Aufgaben . In dieser Ansicht werden die von Ihnen abgeschlossenen Aufgaben mit dem Zeitpunkt der Genehmigung bzw. Ablehnung angezeigt. Um die Details einer abgeschlossenen Aufgabe anzuzeigen, klicken Sie auf die betreffende Aufgabe. Bei komplexeren Anforderungen können Sie auf **Form Values** (Formularwerte) klicken, um spezielle Informationen zu dieser Anforderung anzuzeigen.

Sie können aus dieser Ansicht auch Aufgaben löschen. Zum gleichzeitigen Löschen mehrerer Aufgaben klicken Sie auf das Symbol für den Massenmodus , wählen die Aufgaben aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.

HINWEIS: In der Ansicht mit abgeschlossenen Aufgaben werden nur die auf Ihrem Gerät ausgeführten Aufgaben angezeigt. Aufgaben, die in der Benutzeranwendung oder auf einem anderen Gerät, auf dem die Approvals App installiert ist, ausgeführt wurden, werden hier nicht angezeigt.

A.4.5 Ansicht mit Anmeldeeinstellungen

In dieser Ansicht können Sie Ihre Anmeldeeinstellungen anzeigen und ändern.

WARNUNG: Wenn Ihnen Ihr Identity Manager-Administrator einen Link oder QR-Code für die automatische Konfiguration Ihrer App-Einstellungen bereitgestellt hat, empfehlen wir Ihnen, diese Standardeinstellungen nicht zu ändern, es sei denn, Sie werden von Ihrem Administrator ausdrücklich dazu aufgefordert.

A.4.6 Ansicht mit erweiterten Einstellungen

In dieser Ansicht können Sie erweiterte Einstellungen anzeigen und ändern, die festlegen, wie Sie Daten vom Server des rollenbasierten Bereitstellungsmoduls empfangen.

WARNUNG: Wenn Ihnen Ihr Identity Manager-Administrator einen Link oder QR-Code für die automatische Konfiguration Ihrer App-Einstellungen bereitgestellt hat, empfehlen wir Ihnen, diese Standardeinstellungen nicht zu ändern, es sei denn, Sie werden von Ihrem Administrator ausdrücklich dazu aufgefordert.

Falls Sie die Datendefinitionseinstellungen in der Ansicht mit den erweiterten Einstellungen versehentlich geändert haben, klicken Sie auf **Restore Defaults** (Standardwerte wiederherstellen), um die von Identity Manager bereitgestellten Standardwerte wiederherzustellen. Ihr Benutzername, Passwort und die Serverdetaileinstellungen sind von einer Rücksetzung auf die Standardwerte nicht betroffen.

A.5 Ändern der Anzeigesprache der Approvals App

Die Approvals App beinhaltet in zahlreiche andere Sprachen lokalisierte Textzeichenfolgen ihrer Benutzeroberfläche. Zum Ändern der Anzeigesprache der Approvals App müssen Sie lediglich die Sprach- und Regionseinstellungen Ihres iOS-Geräts ändern. Die Regionseinstellungen legen fest, wie Datums- und Zeitangaben wie auch Telefonnummern auf dem Gerät angezeigt werden.

So ändern Sie die Sprach- und Regionseinstellungen:

1. Klicken Sie auf Ihrem iOS-Gerät auf **Einstellungen**.
2. Klicken Sie auf **Allgemein**.
3. Klicken Sie auf **International**.
4. (Optional) Wenn Sie die Sprache Ihres Geräts ändern möchten, klicken Sie auf **Sprache**, wählen Sie die gewünschte Sprache aus und klicken Sie auf **Fertig**.
5. (Optional) Wenn Sie das regionale Format ändern möchten, das Ihr Gerät für Datums- und Zeitangaben verwendet, klicken Sie auf **Region**, wählen Sie das gewünschte Format aus und klicken Sie auf **International**.
6. Kehren Sie zum Startbildschirm Ihres Geräts zurück.

B Verwenden der Verzeichnissuche in der Benutzeranwendung

In diesem Abschnitt wird erläutert, wie Sie die Seite „Verzeichnissuche“ auf der Registerkarte **Identitätsselbstbedienung** der Benutzeranwendung verwenden. Es werden u. a. folgende Themen erläutert:

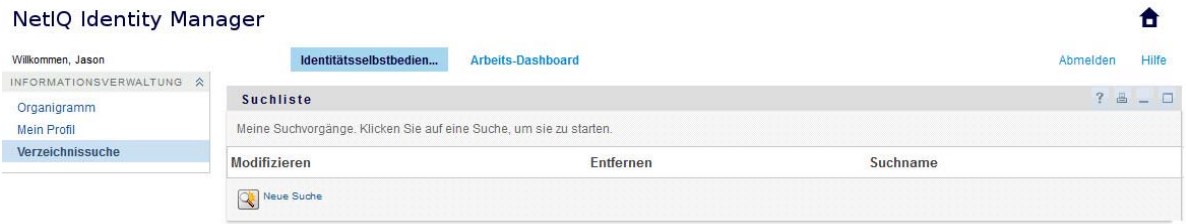
HINWEIS: In diesem Abschnitt werden die Standardfunktionen der Seite „Verzeichnissuche“ beschrieben. Es ist möglich, dass Sie einige Unterschiede zwischen Ihrer Anwendung und den Beschreibungen in diesem Handbuch feststellen. Diese hängen mit Ihrer Rolle und Ihrer hierarchischen Position in der Organisation sowie mit möglichen organisationsbezogenen Anpassungen zusammen. Weitere Informationen erhalten Sie von Ihrem Systemadministrator.

B.1 Grundlagen der Verzeichnissuche

Sie können die Seite „Verzeichnissuche“ zum Suchen von Benutzern, Gruppen oder Teams verwenden. Geben Sie hierzu Suchkriterien ein oder verwenden Sie zuvor gespeicherte Suchkriterien.

Im folgenden Beispiel muss Timothy Swan (Marketing Director) Informationen über einen Mitarbeiter in seiner Organisation suchen. Er ruft die Seite „Verzeichnissuche“ auf. Standardmäßig wird Folgendes wird angezeigt:

Abbildung B-1 *Seite „Verzeichnissuche“*



Da er noch keine Suchkriterien gespeichert hat, wählt er **Neue Suche**.

Er sucht nach einem Benutzer, dessen Vorname mit „C“ beginnt, kann sich aber nicht an den vollen Namen erinnern. Hierzu muss er nur eine einfache Suche mit folgendem Suchkriterium durchführen.

Timothy kann nun die angezeigten Suchergebnisse prüfen und damit arbeiten. Standardmäßig werden die Informationen der Registerkarte **Identität** angezeigt.

Timothy klickt auf die Registerkarte **Organisation**, um eine andere Ansicht der Suchergebnisse zu erhalten. Er erinnert sich, dass die gesuchte Person für Kip Keller arbeitet. Dies grenzt die Suche auf Cal Central ein.

Neben den Registerkarten für unterschiedliche Ansichten enthält die Seite mit den Suchergebnissen Links und Schaltflächen zur Durchführung von Aktionen mit den Informationen. Sie haben folgende Möglichkeiten:

- Die Informationen durch Klicken auf die Spaltenüberschriften sortieren
- Details (Profilseite) zu einem Benutzer oder einer Gruppe durch Klicken auf die entsprechende Zeile anzeigen
- Eine neue Email-Nachricht an einen Benutzer durch Klicken auf das Email-Symbol in der entsprechenden Zeile senden
- Die Sucheinstellungen für die künftige erneute Verwendung speichern
- Die Ergebnisse in eine Textdatei exportieren
- Die Suche durch Ändern der Kriterien anpassen

Zum Generieren von Suchergebnissen genügt mitunter die einfache Suche nicht, um die gewünschten Informationen zu beschreiben. In diesen Fällen können Sie die erweiterte Suche verwenden, um komplexe Suchkriterien anzugeben.

Wenn Sie eine erweiterte Suche möglicherweise erneut durchführen müssen, können Sie sie speichern. Gespeicherte Suchvorgänge sind auch für häufig durchgeführte einfache Suchen hilfreich. Timothy Swan hat beispielsweise mehrere Suchvorgänge gespeichert, die er häufig durchführt.

B.2 Durchführen einfacher Suchvorgänge

1. Rufen Sie die Seite „Verzeichnissuche“ auf und klicken Sie auf **Neue Suche**. Die Seite „Einfache Suche“ wird angezeigt.
2. Wählen Sie in der Dropdown-Liste **Suchen nach** die Art der gesuchten Informationen aus: **Gruppe** oder **Benutzer**.
3. Wählen Sie in der Dropdown-Liste **Elementkategorie** ein Suchattribut aus. Beispiel:

   ```
   Last Name
   ```

   Welche Attribute in der Liste verfügbar sind, hängt vom gewählten Suchkriterium (Benutzer oder Gruppe) ab.
4. Wählen Sie in der Dropdown-Liste **Ausdruck** einen Ausdruck aus, der auf die Suche nach dem von Ihnen ausgewählten Attribut angewandt werden soll. Beispiel:

   ```
   equals
   ```

   Weitere Informationen finden Sie in Abschnitt B.3.1, „Auswahl eines Ausdrucks“, auf Seite 89.
5. Geben Sie im Eingabefeld **Suchbegriff** den Wert ein, nach dem unter Berücksichtigung der vorher festgelegten Attribute gesucht werden soll. Beispiel:

   ```
   Smith
   ```

   Weitere Informationen finden Sie in Abschnitt B.3.2, „Angabe eines Werts für Ihren Vergleich“, auf Seite 90.
6. Klicken Sie auf **Suchen**.

Die Suchergebnisse werden angezeigt.

Informationen über die nächsten auszuführenden Schritte finden Sie in Abschnitt B.4, „Arbeiten mit Suchergebnissen“, auf Seite 94.

B.3 Durchführen erweiterter Suchvorgänge

Wenn Sie mehrere Kriterien für die Suche nach Benutzern oder Gruppen angeben müssen, können Sie die erweiterte Suche verwenden. Beispiel:

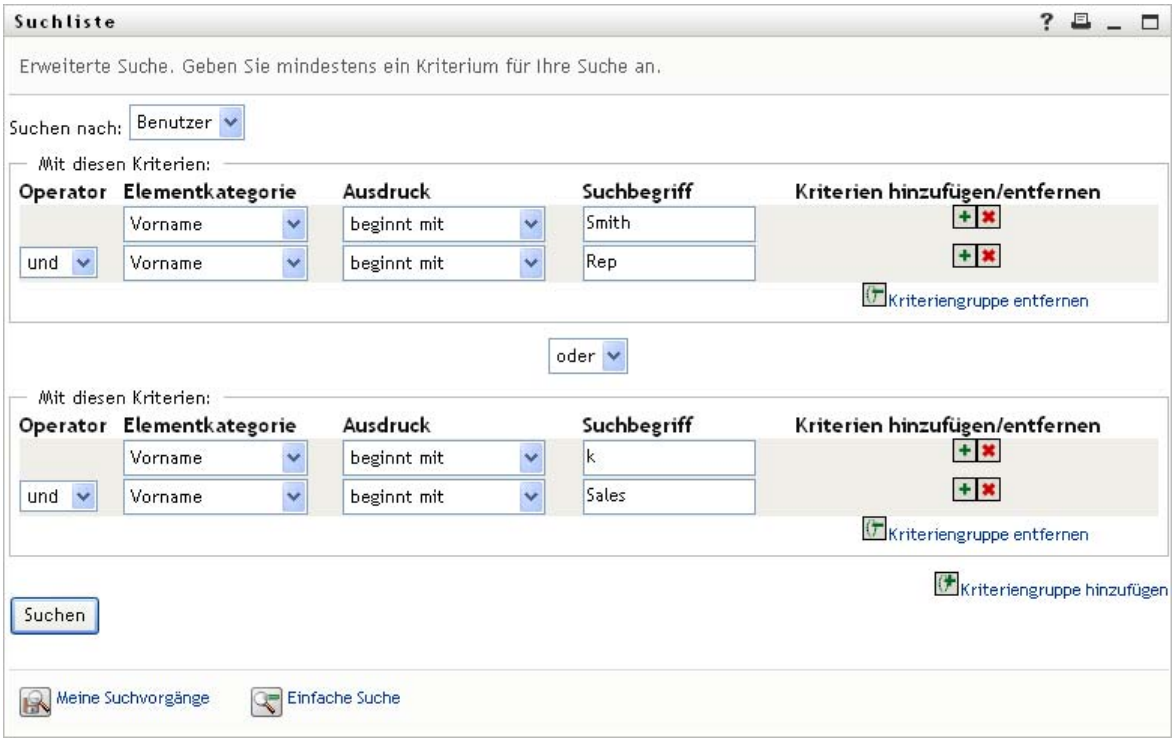
```
Last Name equals Smith AND Title contains Rep
```

Wenn Sie mehrere Kriteriengruppen angeben (um die Reihenfolge der Auswertung der Kriterien zu steuern), wenden Sie dieselben logischen Operatoren an, um sie miteinander zu verbinden. Führen Sie beispielsweise eine erweiterte Suche mit den folgenden Kriterien durch (zwei durch „oder“ verbundene Kriteriengruppen):

```
(Last Name equals Smith AND Title contains Rep) OR (First Name starts with k AND
Department equals Sales)
```

Geben Sie hierzu Folgendes an, siehe Abbildung B-2 auf Seite 87:

Abbildung B-2 *Angabe einer erweiterten Suche auf der Seite „Suchliste“*



Das Suchergebnis wird in Abbildung B-3 auf Seite 88 dargestellt.

Abbildung B-3 *Ergebnis einer erweiterten Suche*

So führen Sie eine erweiterte Suche durch:

1. Rufen Sie die Seite „Verzeichnissuche“ auf und klicken Sie auf **Neue Suche**. Die Seite „Einfache Suche“ wird standardmäßig angezeigt.
2. Klicken Sie auf **Erweiterte Suche**. Die Seite „Erweiterte Suche“ wird angezeigt.
3. Wählen Sie in der Dropdown-Liste **Suchen nach** die Art der gesuchten Informationen durch Auswahl einer der folgenden Optionen aus:
   - Gruppe
   - Benutzer

   Sie können nun den Abschnitt **Mit diesen Kriterien** ausfüllen.
4. Geben Sie ein Kriterium für eine Kriteriengruppe an:

   4a Wählen Sie in der Dropdown-Liste **Elementkategorie** ein Suchattribut aus. Beispiel:

   ```
   Last Name
   ```

   Welche Attribute in der Liste verfügbar sind, hängt vom gewählten Suchkriterium (Benutzer oder Gruppe) ab.

   4b Wählen Sie in der Dropdown-Liste **Ausdruck** einen Operator aus, der auf die Suche nach dem von Ihnen ausgewählten Attribut angewandt werden soll. Beispiel:

   ```
   equals
   ```

   Weitere Informationen finden Sie in Abschnitt B.3.1, „Auswahl eines Ausdrucks“, auf Seite 89.

   4c Geben Sie im Eingabefeld **Suchbegriff** den Wert ein, nach dem unter Berücksichtigung der vorher festgelegten Attribute gesucht werden soll. Beispiel:

   ```
   Smith
   ```

   Weitere Informationen finden Sie in Abschnitt B.3.2, „Angabe eines Werts für Ihren Vergleich“, auf Seite 90.

5 So geben Sie ein weiteres Kriterium einer Kriteriengruppe ein:

5a Klicken Sie auf der rechten Seite der Kriteriengruppe auf **Kriterien hinzufügen**:

5b Verwenden Sie auf der linken Seite des neuen Kriteriums die Dropdown-Liste **Logischer Operator des Kriteriums**, um dieses Kriterium mit dem vorhergehenden zu verbinden. Wählen Sie entweder **und** oder **oder**. Sie können innerhalb einer Kriteriengruppe nur einen der beiden logischen Operatoren verwenden.

5c Wiederholen Sie diese Schritte und beginnen Sie mit Schritt 4.

Klicken Sie zum Löschen eines Kriteriums rechts davon auf **Kriterien entfernen**: 

6 So geben Sie eine weitere Kriteriengruppe an:

6a Klicken Sie auf **Kriteriengruppe hinzufügen**.

6b Verwenden Sie die Dropdown-Liste **Logischer Operator der Kriteriengruppe** oberhalb der Kriteriengruppe, um diese mit der vorherigen zu verbinden. Wählen Sie entweder **und** oder **oder**.

6c Wiederholen Sie diese Schritte und beginnen Sie mit Schritt 4.

Zum Löschen einer Kriteriengruppe klicken Sie direkt darüber auf **Kriteriengruppe entfernen**.

7 Klicken Sie auf **Suchen**.

Die Suchergebnisse werden angezeigt.

Informationen über die nächsten auszuführenden Schritte finden Sie in Abschnitt B.4, „Arbeiten mit Suchergebnissen“, auf Seite 94.

B.3.1 Auswahl eines Ausdrucks

Klicken Sie auf **Ausdruck**, um ein Vergleichskriterium für Ihre Suche auszuwählen. Die Liste der für ein Kriterium verfügbaren (relationalen) Vergleichsoperatoren hängt von dem in diesem Kriterium festgelegten Attributtyp ab:

Tabelle B-1 *Vergleichsoperatoren für die Suche*

Attributtyp	Verfügbare Vergleichsoperatoren
Zeichenkette (Text)	◆ beginnt mit ◆ enthält ◆ gleich ◆ endet mit ◆ ist vorhanden ◆ beginnt nicht mit ◆ enthält nicht ◆ nicht gleich ◆ endet nicht mit ◆ ist nicht vorhanden

Attributtyp	Verfügbare Vergleichsoperatoren
Zeichenkette (Text) mit einer vordefinierten Auswahlliste Benutzer oder Gruppe (oder anderes von DN identifiziertes Objekt) Boolescher Wert (wahr oder falsch)	◆ gleich ◆ ist vorhanden ◆ nicht gleich ◆ ist nicht vorhanden
Benutzer (Elementkategorie: Manager, Gruppe oder Direkt unterstellt)	◆ gleich ◆ ist vorhanden ◆ nicht gleich ◆ ist nicht vorhanden
Gruppe (Elementkategorie: Mitglieder)	◆ gleich ◆ ist vorhanden ◆ nicht gleich ◆ ist nicht vorhanden
Uhrzeit (im Datum-Zeit- oder Nur-Datum-Format) Nummer (Ganzzahl)	◆ gleich ◆ größer als ◆ größer gleich ◆ kleiner als ◆ kleiner oder gleich ◆ ist vorhanden ◆ nicht gleich ◆ nicht größer als ◆ nicht größer oder gleich ◆ nicht kleiner als ◆ nicht kleiner oder gleich ◆ ist nicht vorhanden

B.3.2 Angabe eines Werts für Ihren Vergleich

Die Art des in einem Kriterium angegebenen Attributs legt auch fest, wie Sie den Vergleichswert für dieses Kriterium angeben müssen:

Tabelle B-2 *Eingabemethode für Vergleichswerte*

Attributtyp	Wert wie folgt angeben
Zeichenkette (Text)	Geben Sie den Text in das Textfeld ein, das auf der rechten Seite angezeigt wird.
Zeichenkette (Text) mit einer vordefinierten Auswahlliste	Wählen Sie eine Option in der Dropdown-Liste aus, die auf der rechten Seite angezeigt wird.

Attributtyp	Wert wie folgt angeben
Benutzer oder Gruppe (oder anderes von DN identifiziertes Objekt)	Verwenden Sie die Schaltflächen **Nachschlagen, Verlauf** und **Zurücksetzen**, die auf der rechten Seite angezeigt werden.
Uhrzeit (im Datum-Zeit- oder Nur-Datum-Format)	Verwenden Sie die Schaltflächen **Kalender** und **Zurücksetzen**, die auf der rechten Seite angezeigt werden.
Nummer (Ganzzahl)	Geben Sie die Nummer in das Textfeld ein, das auf der rechten Seite angezeigt wird.
Boolescher Wert (wahr oder falsch)	Geben Sie `wahr` oder `falsch` in das Textfeld ein, das auf der rechten Seite angezeigt wird.

Geben Sie bei folgenden Vergleichsvorgängen keinen Wert an:

- ist vorhanden
- ist nicht vorhanden

Groß-/Kleinschreibung

Bei Textsuchvorgängen wird die Groß-/Kleinschreibung nicht berücksichtigt. Sie erhalten unabhängig von der Schreibweise (Groß-/Kleinschreibung) des Suchbegriffs immer dieselben Ergebnisse. Folgende Begriffe liefern beispielsweise dieselben Ergebnisse:

```
McDonald
```

```
mcdonald
```

```
MCDONALD
```

Platzhalter

Sie können in Ihrem Text auch das Sternchen (*) als Platzhalter verwenden, das für null bzw. mehrere beliebige Zeichen steht. Beispiel:

```
Mc*
```

```
*Donald
```

```
*Don*
```

```
McD*d
```

Verwenden der Schaltflächen „Nachschlagen“, „Verlauf“ und „Zurücksetzen“

Bei einigen Suchkriterien werden die Schaltflächen „Nachschlagen“, „Verlauf“ und „Zurücksetzen“ angezeigt. In diesem Abschnitt wird die Verwendung dieser Schaltflächen beschrieben:

Tabelle B-3 Schaltflächen „Nachschlagen“, „Verlauf“ und „Zurücksetzen“ in Suchkriterien

Schaltfläche	Funktion
	Sucht einen für einen Vergleich zu verwendenden Wert
	Zeigt eine **Verlaufsliste** mit für einen Vergleich verwendeten Werten an
	Setzt den Wert für einen Vergleich zurück

So suchen Sie einen Benutzer:

1 Klicken Sie auf **Nachschlagen** rechts von einem Eintrag (für den Sie einen Benutzer suchen möchten):

Die Suchseite wird angezeigt.

2 Geben Sie Suchkriterien für den gewünschten Benutzer ein:

2a Wählen Sie in der Dropdown-Liste aus, ob die Suche anhand des **Vornamens** oder des **Nachnamens** erfolgen soll.

2b Geben Sie im Textfeld neben der Dropdown-Liste den vollständigen Namen oder einen Teil des Namens ein.

Es werden alle Namen gefunden, die mit dem von Ihnen eingegebenen Text beginnen. Bei der Suche wird die Groß-/Kleinschreibung nicht berücksichtigt. Sie können in Ihrem Text auch das Sternchen (*) als Platzhalter verwenden, das für null bzw. mehrere beliebige Zeichen steht.

Beispielsweise wird mit allen folgenden Suchkriterien der Vorname Chip gefunden:

```
Chip
chip
c
c*
*p
*h*
```

3 Klicken Sie auf **Suchen**.

Auf der Suchseite werden Ihre Suchergebnisse angezeigt.

Wenn die angezeigte Liste mit Benutzern den gesuchten Benutzer enthält, fahren Sie mit Schritt 4 fort. Andernfalls kehren Sie zu Schritt 2 zurück.

Sie können die Suchergebnisse in auf- oder absteigender Reihenfolge sortieren, indem Sie auf die Spaltenüberschriften klicken.

4 Wählen Sie den gewünschten Benutzer in der Liste aus.

Die Suchseite wird geschlossen und der Name des Benutzers wird als zu verwendender Vergleichswert im entsprechenden Eintrag eingetragen.

So suchen Sie eine Gruppe:

1 Fügen Sie **Gruppe** als Suchkriterium hinzu und klicken Sie auf **Nachschlagen** rechts neben dem Feld **Suchbegriff.**

Auf der Suchseite werden Suchergebnisse angezeigt.

2 Geben Sie Suchkriterien für die gewünschte Gruppe ein:

2a In der Dropdown-Liste können Sie für die Suche nur **Beschreibung** auswählen.

2b Geben Sie im Textfeld neben der Dropdown-Liste die vollständige Beschreibung oder einen Teil der Beschreibung ein.

Es werden alle Beschreibungen gefunden, die mit dem von Ihnen eingegebenen Text beginnen. Bei der Suche wird die Groß-/Kleinschreibung nicht berücksichtigt. Sie können in Ihrem Text auch das Sternchen (*) als Platzhalter verwenden, das für null bzw. mehrere beliebige Zeichen steht.

Mit den folgenden Suchkriterien wird beispielsweise die Beschreibung „Marketing“ gefunden:

```
Marketing
marketing
m
m*
*g
*k*
```

3 Klicken Sie auf **Suchen**.

Auf der Suchseite werden Ihre Suchergebnisse angezeigt.

Wenn die angezeigte Liste mit Gruppen die gesuchte Gruppe enthält, fahren Sie mit Schritt 4 fort. Andernfalls kehren Sie zu Schritt 2 zurück.

Sie können die Suchergebnisse in auf- oder absteigender Reihenfolge sortieren, indem Sie auf die Spaltenüberschrift klicken.

4 Wählen Sie die gewünschte Gruppe in der Liste aus.

Die Suchseite wird geschlossen und die Beschreibung dieser Gruppe wird als zu verwendender Vergleichswert in den entsprechenden Eintrag eingetragen.

So verwenden Sie die Liste **Verlauf**:

1 Klicken Sie auf **Verlauf** rechts neben einem Eintrag (dessen vorherige Werte Sie anzeigen möchten):

Die Liste **Verlauf** zeigt zuvor verwendete Werte für dieses Kriterium in alphabetischer Reihenfolge an.

2 Führen Sie einen der folgenden Vorgänge aus:

Um Folgendes zu erzielen	Führen Sie diese Schritte aus
In der Liste **Verlauf** auswählen	Wählen Sie einen Wert in der Liste aus. Die Liste **Verlauf** wird geschlossen und dieser Wert wird als zu verwendender Vergleichswert im entsprechenden Eintrag eingetragen.
Liste **Verlauf** löschen	Klicken Sie auf **Verlauf löschen**. Die Liste **Verlauf** wird geschlossen und die Werte für diesen Eintrag werden gelöscht. Der aktuelle Wert des Eintrags im Vergleichsvorgang wird durch das Löschen der Liste **Verlauf** nicht gelöscht.

B.4 Arbeiten mit Suchergebnissen

In diesem Abschnitt wird erläutert, wie Sie mit Suchergebnissen arbeiten:

- Abschnitt B.4.1, „Allgemeines zu Suchergebnissen“, auf Seite 94
- Abschnitt B.4.2, „Verwenden der Suchliste“, auf Seite 94
- Abschnitt B.4.3, „Weitere Aktionen, die Sie durchführen können“, auf Seite 95

B.4.1 Allgemeines zu Suchergebnissen

Der Inhalt der Suchergebnisse hängt von der Art der durchgeführten Suche ab:

- „Benutzersuche“, auf Seite 94
- „Gruppensuche“, auf Seite 94

Auf jeder Seite mit Suchergebnissen stehen Ihnen folgende Funktionen zur Verfügung:

- Meine Suchvorgänge
- Suche speichern
- Suche revidieren
- Ergebnisse exportieren
- Neue Suche

Benutzersuche

Bei einer Benutzersuche enthält die Suchergebnisliste drei Registerkarten mit Informationen:

- *Identität* (Kontaktdaten)
- *Standort* (geografische Informationen)
- *Organisation* (Informationen zur Organisation)

Gruppensuche

Bei einer Gruppensuche enthält die Suchergebnisliste nur die Informationen zur Organisation.

B.4.2 Verwenden der Suchliste

Sie können Folgendes mit der Liste der Suchergebnisse tun:

- „Zu einer anderen Ansicht wechseln“, auf Seite 95
- „Zeilen sortieren“, auf Seite 95
- „Details zu einem Benutzer oder einer Gruppe anzeigen“, auf Seite 95
- „Email an einen Benutzer in der Suchliste senden“, auf Seite 95

Zu einer anderen Ansicht wechseln

1 Klicken Sie auf die Registerkarte, die Sie anzeigen möchten.

Zeilen sortieren

1 Klicken Sie auf die Überschrift der Spalte, nach der Sie sortieren möchten.

   Die anfängliche Sortierung erfolgt in aufsteigender Reihenfolge.

2 Sie können zwischen auf- und absteigender Reihenfolge wechseln, indem Sie erneut auf die Spaltenüberschrift klicken (beliebig oft).

Details zu einem Benutzer oder einer Gruppe anzeigen

1 Klicken Sie auf die Zeile des Benutzers oder der Gruppe, zu dem bzw. der Sie Details anzeigen möchten (klicken Sie nicht direkt auf das Email-Symbol, es sei denn, Sie möchten eine Nachricht senden).

   Die Seite „Profil“ wird angezeigt. Sie enthält detaillierte Informationen zum ausgewählten Benutzer bzw. zur Gruppe.

   Diese Seite entspricht der Seite „Mein Profil“ auf der Registerkarte **Identitätsselbstbedienung**. Der einzige Unterschied besteht darin, dass Sie beim Anzeigen von Details eines anderen Benutzers oder einer anderen Gruppe (anders als bei Ihren eigenen Daten) möglicherweise nicht zur Ansicht aller Daten oder zur Durchführung bestimmter Aktionen auf der Seite berechtigt sind. Wenden Sie sich an Ihren Systemadministrator, wenn Sie Hilfe benötigen.

2 Wenn Sie mit der Profilseite fertig sind, können Sie das Fenster schließen.

Email an einen Benutzer in der Suchliste senden

1 Suchen Sie die Zeile des Benutzers, dem Sie eine Email senden möchten.

2 Klicken Sie auf **Email senden** in der Zeile des gewünschten Benutzers:

   Es wird eine neue Nachricht in Ihrem Standard-Email-Client erstellt. Die Nachricht ist leer bis auf das Feld **An**, in dem bereits der von Ihnen ausgewählte Benutzer als Empfänger angegeben ist.

3 Geben Sie den Nachrichtentext ein.

4 Senden Sie die Nachricht.

B.4.3 Weitere Aktionen, die Sie durchführen können

Bei der Anzeige von Suchergebnissen haben Sie folgende weitere Möglichkeiten:

- „Suche speichern“, auf Seite 95
- „Suchergebnisse exportieren“, auf Seite 96
- „Suchkriterien revidieren“, auf Seite 97

Suche speichern

So speichern Sie den aktuellen Satz an Suchkriterien zur künftigen Wiederverwendung:

1 Klicken Sie auf **Suche speichern** (unten auf der Seite).

2 Geben Sie bei Aufforderung einen Namen für diese Suche ein.

Wenn Sie die Ergebnisse einer gespeicherten Suche anzeigen, wird standardmäßig dieser Suchname angezeigt. So können Sie eine gespeicherte Suche aktualisieren, wenn Sie Änderungen an den Suchkriterien vorgenommen haben.

Falls Sie einen Namen eingeben, der bereits für eine gespeicherte Suche vergeben ist, wird automatisch eine Versionsnummer an den Namen angehängt, wenn Sie die neue Suche speichern.

3 Klicken Sie auf **OK**, um die Suche zu speichern.

Auf der Seite „Suchliste“ wird die Liste „Meine Suchvorgänge“ angezeigt.

Weitere Informationen zum Arbeiten mit gespeicherten Suchvorgängen finden Sie in Abschnitt B.5, „Verwenden gespeicherter Suchvorgänge“, auf Seite 97.

Suchergebnisse exportieren

So exportieren Sie Suchergebnisse in eine Textdatei:

1 Klicken Sie auf **Ergebnisse exportieren** (unten auf der Seite).

Die Seite „Exportieren“ wird angezeigt.

Standardmäßig ist **Auf dem Bildschirm ansehen** ausgewählt und **CSV** ist als Format in der entsprechenden Dropdown-Liste angegeben. So werden Ihre Suchergebnisse auf der Seite „Exportieren“ im CSV-Format (Comma Separated Value) angezeigt.

2 Wenn Sie die Suchergebnisse im tabulatorgetrennten Format anzeigen möchten, wählen Sie **Tabulatorgetrennt** in der Dropdown-Liste aus und klicken Sie auf **Weiter**.

3 Wählen Sie **Auf Datenträger exportieren**, um die aktuellen Suchergebnisse in eine Textdatei zu exportieren.

Die Seite „Exportieren“ wird angezeigt.

4 Wählen Sie in der Dropdown-Liste **Format** das Exportformat für die Suchergebnisse aus.

Exportformat	Standardname der generierten Datei
CSV	SearchListResult.*Datum*.*Uhrzeit*.csv Beispiel: `SearchListResult.27-Sep-05.11.21.47.csv`
Tabulatorgetrennt	SearchListResult.*Datum*.*Uhrzeit*.txt Beispiel: `SearchListResult.27-Sep-05.11.20.51.txt`
XML (beim Exportieren auf einen Datenträger verfügbar)	SearchListResult.*Datum*.*Uhrzeit*.xml Beispiel: `SearchListResult.27-Sep-05.11.22.51.xml`

5 Klicken Sie auf **Exportieren**.

6 Geben Sie bei Aufforderung den Speicherort der Datei mit den exportierten Suchergebnissen an.

7 Klicken Sie nach dem Export auf **Fenster schließen**.

Suchkriterien revidieren

1 Klicken Sie auf **Suche revidieren** (unten auf der Seite).

Daraufhin wird die vorherige Suchseite angezeigt, auf der Sie die Suchkriterien bearbeiten können.

2 Nehmen Sie die Änderungen an den Suchkriterien wie in den folgenden Abschnitten beschrieben vor:

- Abschnitt B.2, „Durchführen einfacher Suchvorgänge“, auf Seite 86
- Abschnitt B.3, „Durchführen erweiterter Suchvorgänge“, auf Seite 87

B.5 Verwenden gespeicherter Suchvorgänge

Wenn Sie zur „Verzeichnissuche“ wechseln, wird standardmäßig die Seite „Meine Suchvorgänge“ angezeigt. In diesem Abschnitt wird beschrieben, was Sie mit gespeicherten Suchvorgängen tun können:

B.5.1 Gespeicherte Suchvorgänge auflisten

1 Klicken Sie unten auf der Seite „Verzeichnissuche“ auf **Meine Suchvorgänge**. Die Seite „Meine Suchvorgänge“ wird angezeigt.

B.5.2 Gespeicherte Suchvorgänge ausführen

1 Suchen Sie in der Liste **Meine Suchvorgänge** den Suchvorgang aus, den Sie ausführen möchten.

2 Klicken Sie auf den Namen des gespeicherten Suchvorgangs (oder auf den Anfang der Zeile).

Die Suchergebnisse werden angezeigt.

Informationen über die nächsten auszuführenden Schritte finden Sie in Abschnitt B.4, „Arbeiten mit Suchergebnissen“, auf Seite 94.

B.5.3 Gespeicherte Suchvorgänge bearbeiten

1 Suchen Sie in der Liste **Meine Suchvorgänge** den Suchvorgang aus, den Sie bearbeiten möchten.

2 Klicken Sie in der Zeile des gespeicherten Suchvorgangs auf **Bearbeiten**.

Die Seite zum Bearbeiten der Suchkriterien wird angezeigt.

3 Nehmen Sie die Änderungen an den Suchkriterien wie in den folgenden Abschnitten beschrieben vor:

- Abschnitt B.2, „Durchführen einfacher Suchvorgänge“, auf Seite 86
- Abschnitt B.3, „Durchführen erweiterter Suchvorgänge“, auf Seite 87

4 Informationen zum Speichern der Änderungen an der Suche finden Sie in Abschnitt B.4, „Arbeiten mit Suchergebnissen“, auf Seite 94.

B.5.4 Gespeicherte Suchvorgänge löschen

1. Suchen Sie in der Liste **Meine Suchvorgänge** den Suchvorgang aus, den Sie löschen möchten.
2. Klicken Sie auf **Löschen** in der Zeile des gespeicherten Suchvorgangs.
3. Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.