daccord

User Guide

daccord User Frontend

Version 1.6.2

g+hsystems

Ihr Kontakt

G+H Systems GmbH
Professionell, effizient und zuverlässig.

Ludwigstraße 8
63067 Offenbach am Main
Deutschland

Telefon: +49 (0) 69 85 00 02 -0
Fax: +49 (0) 69 85 00 02 -51
Email: info@guh-systems.de
Web: www.guh-systems.de

Versionsnachweis

Dieses Dokument wird von der G+H Systems GmbH gepflegt und fortlaufend aktualisiert. Größere Änderungen an Inhalt und Umfang führen zu einer neuen Versionsnummer. Die folgende Liste gibt die Historie dieses Dokumentes wieder.

Version	Datum	Author	Änderungsgrund
0.5	08.07.2013	Sebastian Kornblueh	Initial Version
1.0	12.09.2013	Sebastian Kornblueh	Finale Version
1.5	30.04.2014	Kevin Bauer und Thomas Gertler	Kompatiblität zu daccord Version 1.5
1.6	02.02.2016	Sebastian Radau	Kompatibilität zu daccord Version 1.6
1.6.2	16.08.2016	Sebastian Radau	Kompatibilität zu daccord Version 1.6.2

Tabelle 1: Versionsübersicht

Rechtliche Hinweise

Die G+H Systems leistet keinerlei Gewähr bezüglich des Inhaltes oder Gebrauchs dieser Dokumentation. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Die G+H Systems behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt die G+H Systems für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich die G+H Systems das Recht vor, G+H Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für die G+H Systems die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Inhaltsverzeichnis

1 Einleitung

Das webbasierte daccord User Frontend dient dem Endanwender zum Zugriff auf die Informationen zu Benutzern und Berechtigungen aus den angeschlossenen Systemen. Je nach Konfiguration des daccord User Frontends, individueller Berechtigung sowie Zuordnung innerhalb des daccord Systems werden ihm die Informationen in folgenden Kategorien dargestellt:

1. Meine Benutzerkonten - Der Anwender erhält eine Darstellung seiner Benutzerkonten und deren Berechtigungen in den verschiedenen Systemen.
2. Meine Rollen - Der Anwender erhält eine Übersicht der Rollen, denen er zugeordnet ist, die Berechtigungen, welche er aufgrund der Zuordnung haben sollte, sowie eine Darstellung der Abweichungen zu den wirklichen Berechtigungszuordnungen.
3. Meine Historie - Der Anwender erhält die Möglichkeit die historischen Daten zu elektronischen Anträgen bezüglich seiner Benutzer, Berechtigungen und Freigaben einzusehen.
4. Personen - Der Anwender erhält eine Darstellung aller Personen, die ihm zugeordnet sind, sowie deren Benutzerkonten, Berechtigungen, Rollen und deren historische Daten.
5. Systeme - Der Anwender erhält eine Darstellung aller Benutzerkonten und Berechtigungen für Systeme, in denen er als Verantwortlicher definiert wurde.
6. Berechtigungen - Der Anwender erhält eine Darstellung der Berechtigungen, für die er als Verantwortlicher definiert wurde. Er kann die Benutzer, die die Berechtigungen besitzen einsehen und eine Rezertifizierung der Zuordnungen durchführen.
7. Rollenmanager - Der Anwender erhält eine Darstellung der Rollen, für die er als Verantwortlicher definiert wurde. Er kann die Berechtigungen, der einzelnen Rollen und deren untergeordneten Rollen einsehen und eine Rezertifizierung der Zuordnungen durchführen.

Desweiteren lassen sich bestimmte Prozesse (z.B. verschicken einer E-Mail, Zugriff auf eine Schnittstelle mit einem Webservice) konfigurieren, die z.B. beim Beantragen einer Löschung, Klärung oder Re-/Zertifizierung von Benutzerkonten und Berechtigungen angestoßen werden können.

Dieser Guide soll Sie bei dem Umgang mit dem daccord User Frontend unterstützen.

Mehr zum daccord System erfahren Sie hier:
http://www.daccord.de

2 daccord User Frontend Allgemein

2.1 daccord User Frontend Anmeldung

Um sich am daccord User Frontend anmelden zu können, geben Sie in einem beliebigen Web-Browser (Mozilla Firefox, Microsoft Internet Explorer, Google Chrome) die Adresse Ihres daccord Servers mit der Endung „/user/" ein, beispielsweise:

```
www.mein-daccord-server.de/user/
```

Sie gelangen auf die Anmelde-Maske. Geben Sie hier Ihren Benutzernamen und Ihr Passwort ein, um sich am daccord User Frontend anzumelden. Je nach Konfiguration des daccord User Frontend ist es möglich, sich über die Netzwerk-Anmeldeinformationen oder über die in daccord hinterlegten Anmeldeinformationen anzumelden.

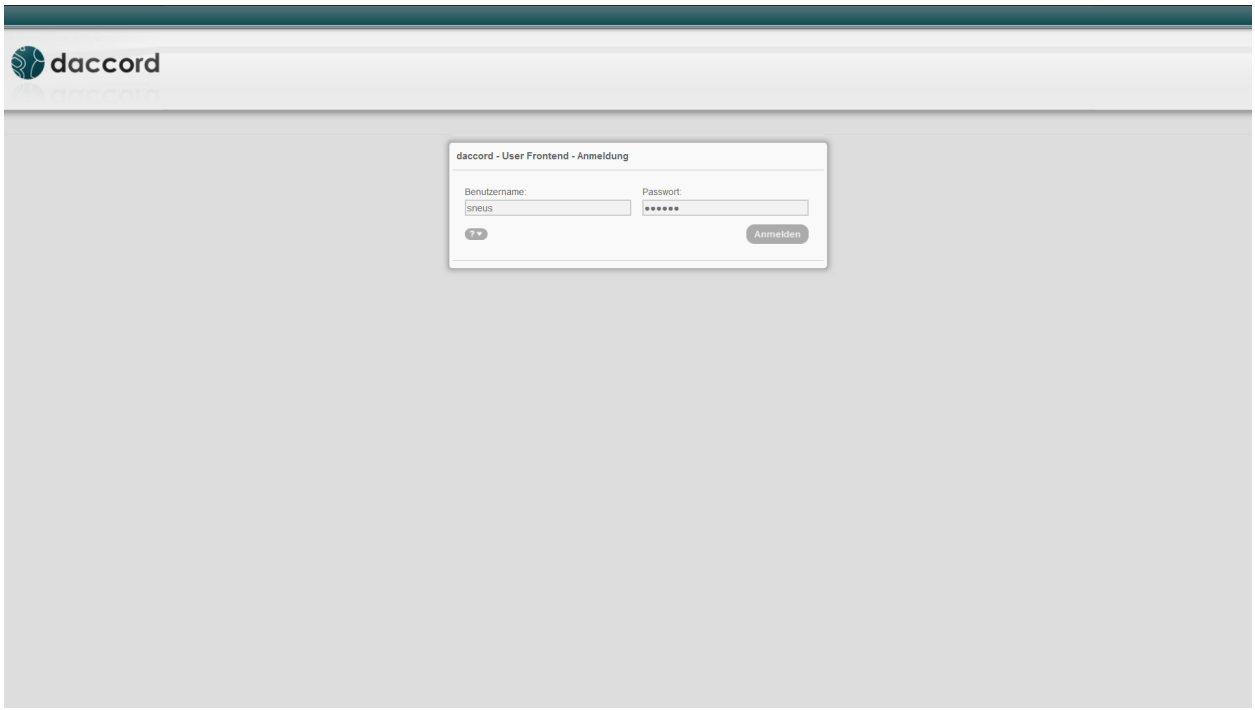


Abbildung 1: Anmeldung am daccord User Frontend

2.2 daccord User Frontend Kopfzeile

Nach der erfolgreichen Anmeldung am daccord User Frontend wird die Auswahl von verschiedenen Ansichten und Einstellungsmöglichkeiten angeboten.

Im oberen, rechten Bereich (Meta-Navigation) der daccord User Frontend befinden sich folgende Schnellzugriffe:

1. Über daccord - Zeigt Ihnen an, welche daccord User Frontend Version aktuell auf Ihrem System verwendet wird.
2. Sie sind angemeldet als: - Zeigt Ihnen an, mit welchem Benutzerkonto Sie gegenwärtig am daccord User Frontend angemeldet sind.
3. Nachrichten - Zeigt an, ob Sie Nachrichten vom daccord System erhalten haben. Benutzen Sie diese Funktion um die Nachrichten einzusehen.
4. English/Deutsch - Schalten Sie zwischen den Sprachen Englisch und Deutsch um.
5. Abmelden - Benutzen Sie diese Funktion, um sich vom daccord User Frontend abzumelden.

2.3 daccord User Frontend Personendaten

Im Bereich „Personendaten" werden ausführliche Informationen über aktuell angemeldete Person angezeigt.

Hinweis: *Sollten Sie über den Vertretungs- oder Administratormodus auf eine andere Person zugreifen, sehen Sie in den ‚Personendaten" die Detail-Informationen zu dem jeweiligen User.*

Parameter	Beschreibung
Vorname	Vorname der angemeldeten Person.
Nachname	Nachname der angemeldeten Person.
Telefon	Telefonnummer der angemeldeten Person, sofern eine hinterlegt wurde.
Email	Emailadresse der angemeldeten Person, sofern eine hinterlegt wurde.
Standort	Ort, an dem die Person arbeitet, sofern einer hinterlegt wurde.
Kostenstelle	Gibt die Kostenstelle der Person an, sofern eine eingetragen wurde.
Unternehmen	Name des Unternehmens, bei dem die Person angestellt ist, sofern eins hinterlegt wurde.
Personalnummer	Personalnummer der angemeldeten Person, sofern eine hinterlegt wurde.
Abteilung	Gibt an, in welcher Abteilung die angemeldete Person angestellt ist, sofern eine hinterlegt wurde.
Personentyp	Gibt an, ob es sich um einen internen oder externen Mitarbeiter handelt.

Tabelle 2: Personendaten

Hinweis: *Über das -Symbol neben der Auswahl des Vertretungsmodus können Sie das Fenster „Personendaten" ein- und ausblenden.*

2.4 daccord User Frontend Administratormodus

Über den Administratormodus können Sie die Anzeige des daccord User Frontends anderer Personen aufrufen, sofern Sie Zugriff auf deren Daten haben bzw. die notwendigen administrativen daccord Rechte besitzen.

Mit einem Klick auf „Administratormodus" (oben rechts im Bereich der Personendaten) öffnet sich ein neues Fenster, indem die Benutzer aufgelistet werden. Über das „Lupen"-Symbol lässt sich der Administratormodus für den jeweiligen Benutzer einschalten.

Hinweis: *Bei Benutzern, denen kein führendes System zugeordnet ist, wird statt der Lupe ein gelbes Warndreieck angezeigt. Bei diesen Benutzern kann nicht in den Administratormodus gewechselt werden.*

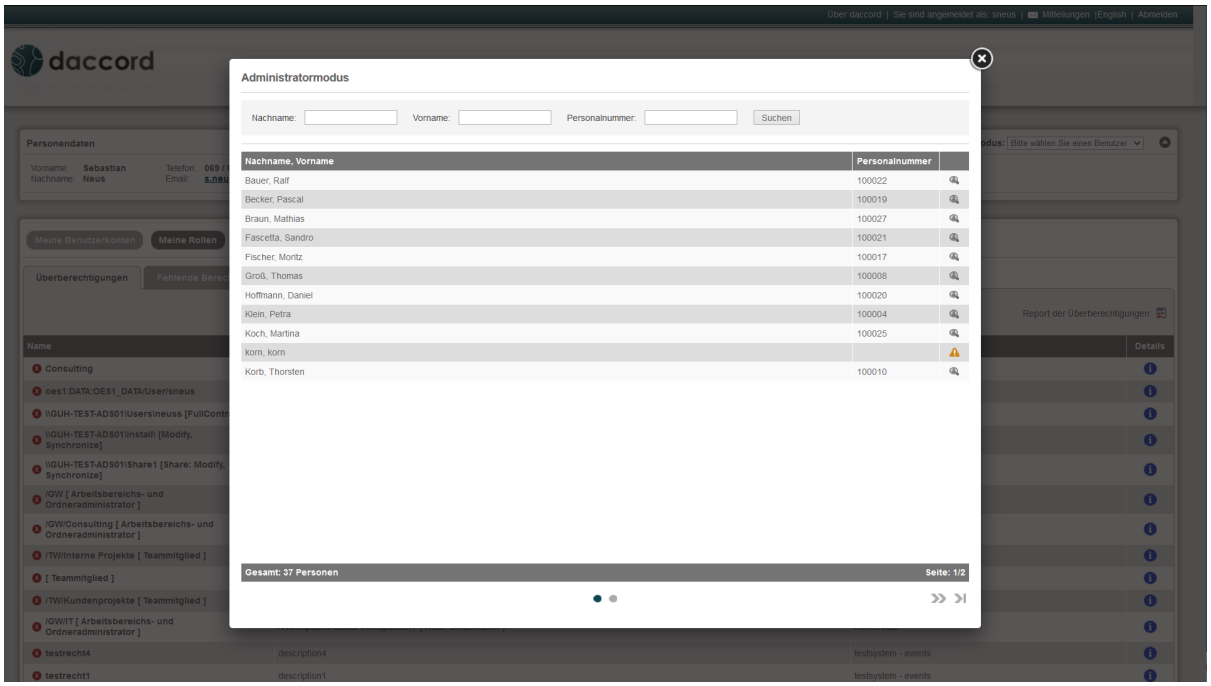


Abbildung 2: Administratormodus - Benutzerübersicht

Solange Sie sich im Administratormodus befinden, wird dies mit einem roten Hinweis, innerhalb der Personendaten angezeigt. Um den Administratormodus wieder abzuschalten, klicken Sie auf den entsprechenden Link am Ende des Hinweises.

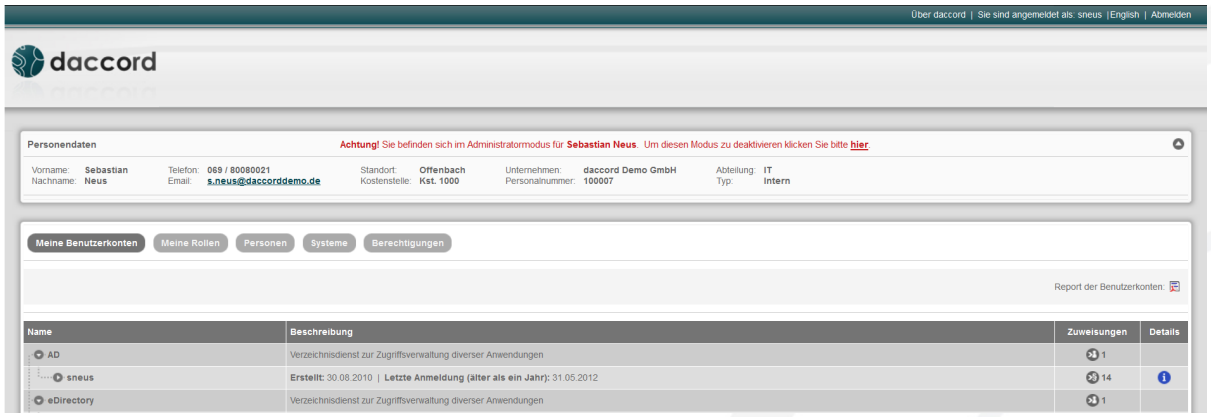


Abbildung 3: Ansicht eines Benutzers im Administratormodus

2.5 daccord User Frontend Vertretungsmodus

In daccord können für einen „Person Manager", „Right Manager", „Role Manager" oder „System Manager" andere Manager als Vetretung konfiguriert werden. Fällt ein Manager z.B. wegen einer Krankheit für längere Zeit aus, kann ein anderer Manager, mit Hilfe des Vetretungsmodus, seine Vertretung übernehmen.

Ähnlich wie der Administratormode ermöglicht es der Vertretungsmodus, die Anzeige des daccord User Frontends einer anderen Person aufzurufen. In einer DropDown-Box werden alle Benutzer angezeigt, für die Sie als Vertretung berechtigt sind. Um in die Ansicht einer anderen Person zu springen, wählen Sie diese einfach aus.

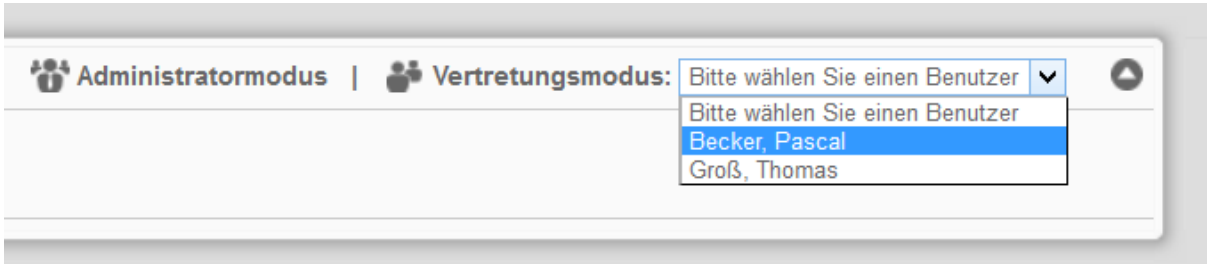


Abbildung 4: DropDown-Menü zum Wechseln in den Vertretungsmodus

Solange Sie sich im Vertretungsmodus befinden, wird dies mit einem roten Hinweis, innerhalb der Personendaten angezeigt. Um den Vertretungsmodus wieder abzuschalten, klicken Sie auf den entsprechenden Link am Ende des Hinweises.

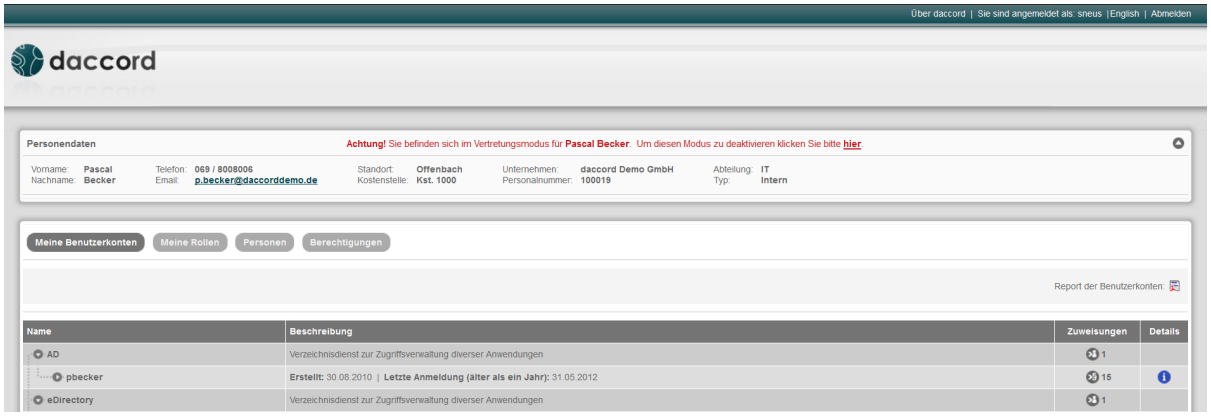


Abbildung 5: Ansicht eines Benutzers im Vertretungsmodus

3 daccord User Frontend Tabs

Im folgenden Abschnitt erhalten Sie eine detaillierte Übersicht über die im daccord User Frontend verfügbaren Tabs „Meine Benutzerkonten", „Meine Rollen", „Meine Historie", „Personen", „Systeme", „Berechtigungen" und „Rollenmanager".

Hinweis: *Die Anzeige der Tabs „Personen", „Systeme" und „Berechtigungen" ist abhängig von der Zuweisung der jeweiligen Verantwortlichkeit („Person Manager", „System Manager", „Right Manager"). Die Tabs „Meine Rollen", „Meine Historie" und „Rollenmanager" werden nur bei Aktivierung der dementsprechenden Module angezeigt. Für detaillierte Informationen kontaktieren Sie bitte Ihren daccord Systemadministrator.*

3.1 Meine Benutzerkonten

Unter „Meine Benutzerkonten" wird eine Übersicht aller Benutzerkonten inkl. der jeweilig zugewiesenen Berechtigungen angeboten, welche die angemeldete Person in den angebundenen Systemen besitzt.

Die Übersicht ist zunächst nach den Systemen sortiert, in welchen die Person Benutzerkonten besitzt. Unter den jeweilige Benutzerkonten können die zugewiesenen Berechtigungen eingesehen werden. Hierbei werden sowohl die Beschreibungen, als auch Erstellungsdaten oder Vergabedaten und historische Einträge zu den jeweiligen Datensätzen angezeigt. Ist das Antragsmodul aktiviert so können die jeweiligen Anträge zu den Benutzeranlagen oder Berechtigungsvergaben dargestellt oder ausgelöst werden.

Sie haben ebenfalls die Möglichkeit, einen Report über ein bestimmtes Benutzerkonto, bzw. einen Report über alle Benutzerkonten der angemeldeten Person zu generieren und als PDF zur Verfügung gestellt zu bekommen.

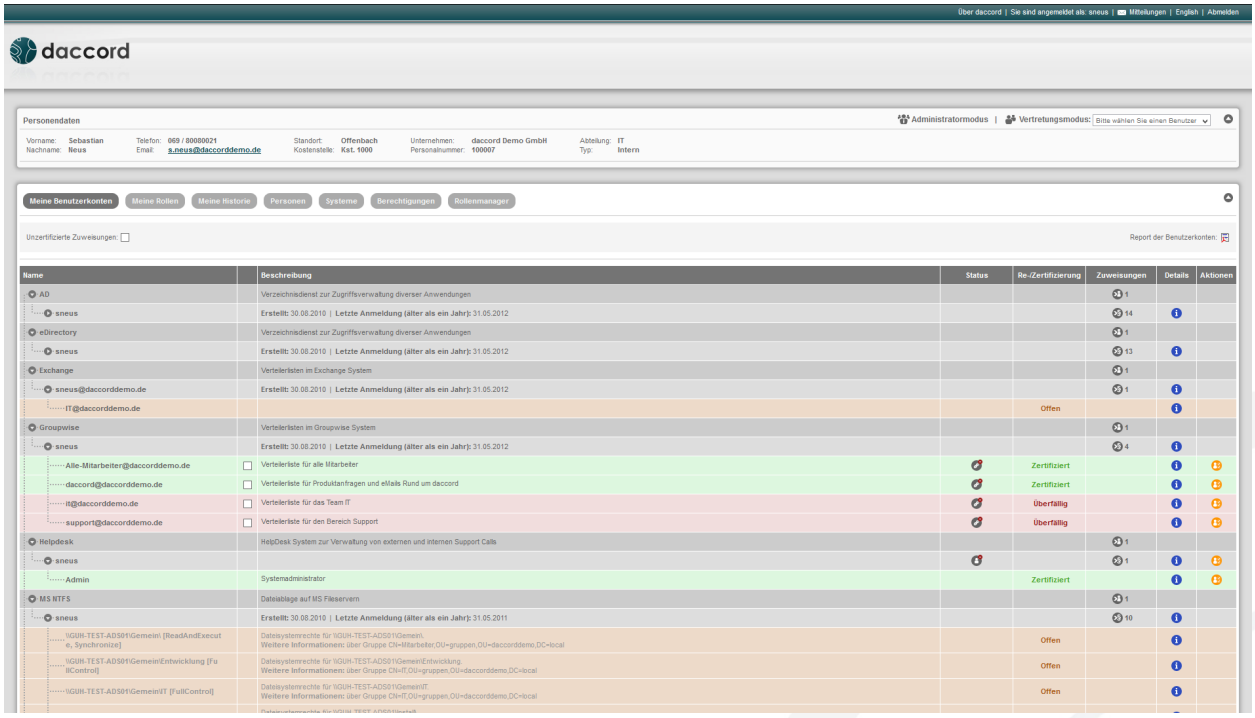


Abbildung 6: Meine Benutzerkonten

Hinweis: *Um einen Report über alle Benutzerkonten der angemeldeten Person zu ziehen, klicken Sie oben rechts oberhalb der Auflistung auf „Report der Benutzerkonten". Daraufhin wird eine PDF generiert und zum Download angeboten.*

In der letzten Spalte „Details" wird je nachdem, wie das daccord User Frontend eingerichtet ist, ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon lassen sich weitere Informationen zu dem ausgewählten Eintrag anzeigen. Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

Ist die Re-/Zertifizierung aktiviert, können je nach Berechtigung, die einzelnen Benutzerkonten re-/zertifiziert werden. Mehr zum Thema Re-/Zertifizierung finden Sie im Kapitel “5.3. Re-/Zertifizierung”.

3.1.1 Erläuterung der Spalte „Status“

In der Spalte Status werden, bereits beantragte, aber noch nicht durchgeführte Aktionen in Form verschiedener Icons angezeigt.

Abbildung 7: Tab: Meine Benutzerkonten

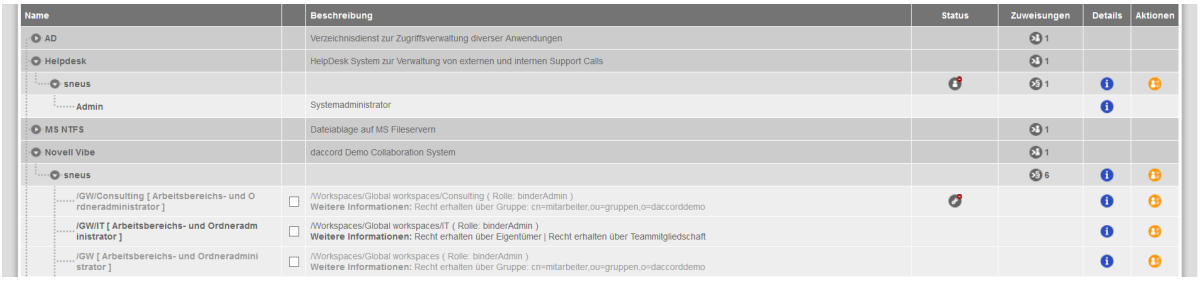
3.1.2 Erläuterung der Spalte „Zuweisungen“

Eine Person kann mehrere Benutzerkonten in einem System haben. Einem Benutzerkonto können wiederum mehrere Berechtigungen zugewiesen sein. Die Anzahl der jeweiligen Zuweisungen wird in der Spalte „Zuweisungen” angezeigt. Neben der Anzahl wird ein Icon eingeblendet, um zu verdeutlichen um welche Art von Zuweisung es sich handelt. Bei zugewiesenen Usern wird ein graues Icon mit einem User angezeigt. Bei zugewiesenen Berechtigungen wird ein Icon mit einem Rechtezeichen angezeigt.

Hinweis: *Sie können sich die zugewiesenen Berechtigungen zum jeweiligen Benutzerkonto anzeigen lassen, indem Sie links auf den entsprechenden Pfeil klicken.*

3.1.3 Erläuterung der Spalte „Beschreibung“

Die Spalte Beschreibung bietet zum Namen eine genauere Beschreibung an. Bei Benutzerkonten wird in dieser Spalte angegeben, wann das Konto erstellt und das letzte mal benutzt wurde. Handelt es sich um eine Berechtigung, kann anhand des Beschreibungstextes abgeleitet werden, ob die Berechtigung direkt, oder indirekt (z.B. über eine Gruppe oder ein Profil) vergeben wurde.



Name		Beschreibung	Status	Zuweisungen	Details	Aktionen
AD		Verzeichnisdienst zur Zugriffsverwaltung diverser Anwendungen		1		
Helpdesk		HelpDesk System zur Verwaltung von externen und internen Support Calls		1		
sneus				1		
Admin		Systemadministrator				
MS NTFS		Dateiablage auf MS Fileservern		1		
Novell Vibe		daccord Demo Collaboration System		1		
sneus				6		
/GW/Consulting [Arbeitsbereichs- und Ordneradministrator]	☐	/Workspaces/Global workspaces/Consulting (Rolle: binderAdmin) **Weitere Informationen:** Recht erhalten über Gruppe: cn=mitarbeiter,ou=gruppen,o=daccorddemo				
/GW/IT [Arbeitsbereichs- und Ordneradministrator]	☐	/Workspaces/Global workspaces/IT (Rolle: binderAdmin) **Weitere Informationen:** Recht erhalten über Eigentümer | Recht erhalten über Teammitgliedschaft				
/GW [Arbeitsbereichs- und Ordneradministrator]	☐	/Workspaces/Global workspaces (Rolle: binderAdmin) **Weitere Informationen:** Recht erhalten über Gruppe: cn=mitarbeiter,ou=gruppen,o=daccorddemo				

Abbildung 8: In dieser Ansicht erkennt man die verschiedenen Beschreibungen

3.2 Meine Rollen

Unter dem Tab "Meine Rollen" werden alle Rollen angezeigt, die dem aktuell angemeldetem Benutzer zugewiesen sind. Zur besseren Übersicht, sind die einzelnen Rollen auf die Untertabs "Überberechtigungen", "Fehlende Berechtigungen" und "Zugewiesene Rollen" unterteilt.

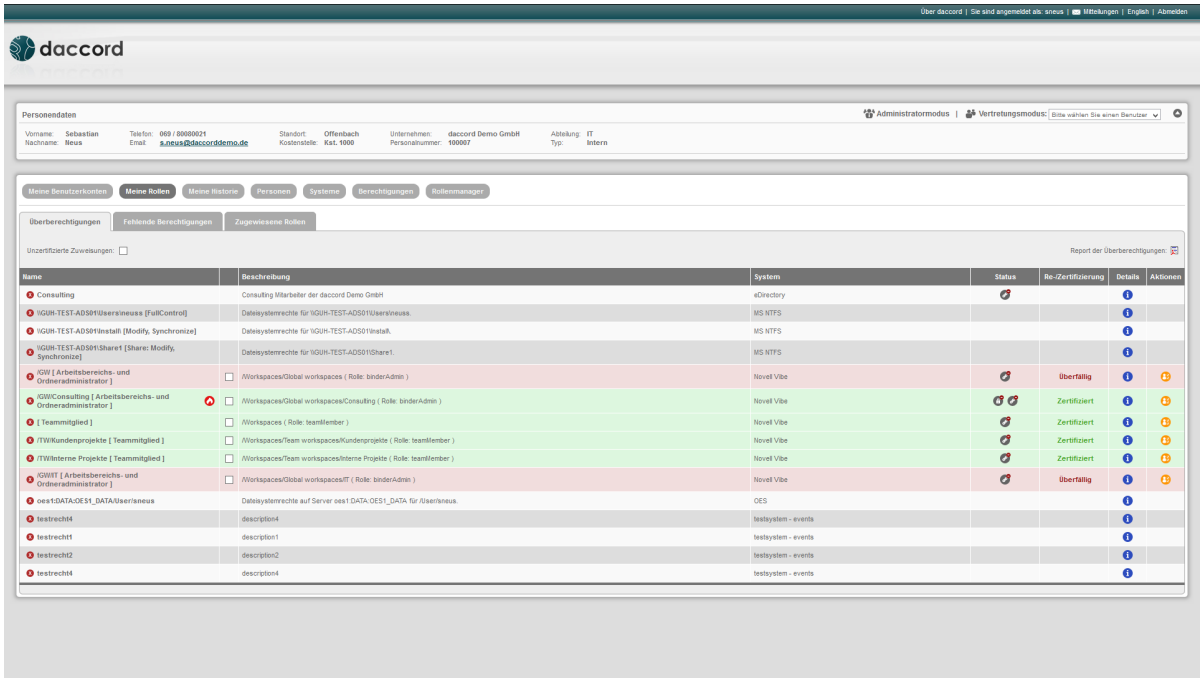


Abbildung 9: Meine Rollen - Überberechtigungen

Beim Aufruf des „Meine Rollen" Tabs wird ein Soll-Ist-Vergleich hinsichtlich der Konformität der importierten Daten (Ist-Stand) zu dem in daccord definierten Rollen-Modell (Soll-Stand) durchgeführt. Je nach Ergebniss des Vergleichs, wird dieser einem der oben genannten Tabs zugewiesen. Eine genauere Beschreibung der Tabs finden Sie in den folgenden Kapiteln.

Hinweis: *Bitte beachten Sie, dass das „Meine Rollen" Tab nur angezeigt wird wenn das Rollenmodul aktiviert ist. Bei Problemen wenden Sie sich bitte an Ihren daccord Systemadministrator.*

In der letzten Spalte „Details" wird je nachdem, wie das daccord User Frontend eingerichtet ist, ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon lassen sich weitere Informationen zu dem ausgewählten Eintrag anzeigen. Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

Ist die Re-/Zertifizierung aktiviert, können je nach Berechtigung, die einzelnen Rollen re-/zertifiziert werden. Mehr zum Thema Re-/Zertifizierung finden Sie im Kapitel "5.3.2. Re-/Zertifizierung von Rollen".

3.2.1 Überberechtigungen

Beim Aufruf des Tabs „Überberechtigungen" findet ein Soll-Ist-Vergleich, hinsichtlich der Konformität der importierten Daten (Ist-Stand) zu dem in daccord definierten Rollen-Modell (Soll-Stand) statt. Wenn eine vom Zielsystem importierte Berechtigungszuweisung existiert, die laut dem Rollenmodell von daccord nicht existieren darf, ist diese Berechtigung zuviel zugewiesen worden. Die Berechtigungszuweisung wird daraufhin unter dem Tab „Überberechtigungen" angezeigt und erhält ein rotes Error-Symbol.

Hinweis: *Lassen Sie sich alle Überberechtigungen der aktuell angemeldeten Person als Report im PDF-Format ausgeben. Klicken Sie dazu auf das PDF-Icon „Report der Überberechtigungen" rechts oberhalb der Tabelle.*

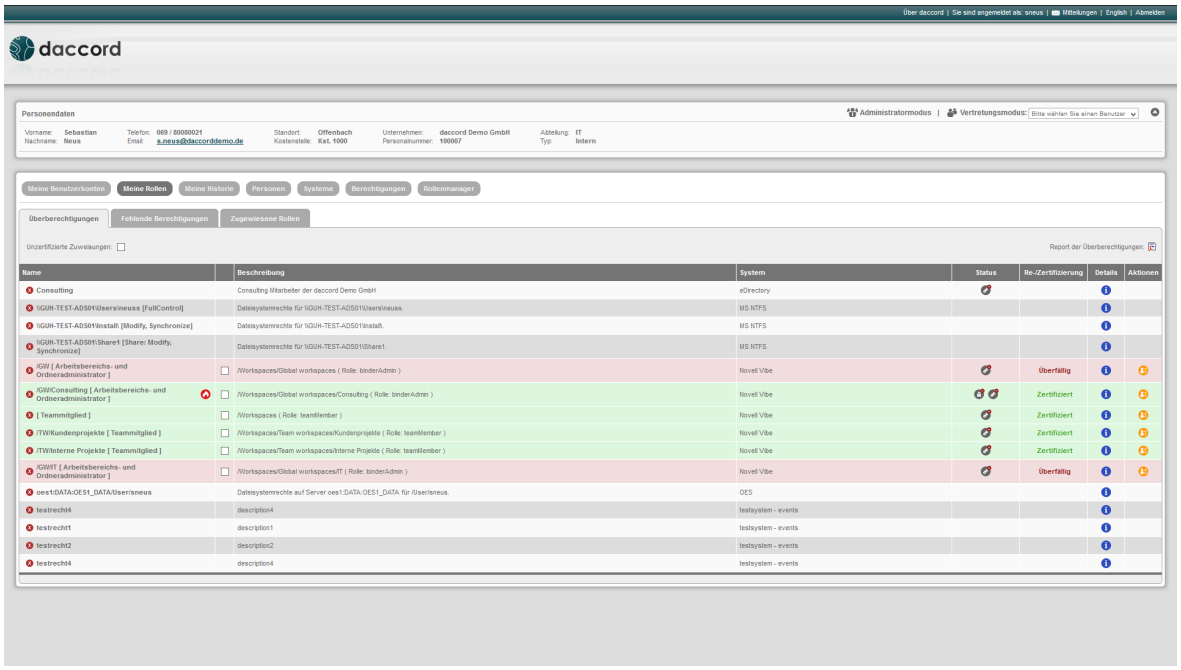


Abbildung 10: Überberechtigungen

Ist die Rollen-Zertifizierung aktiviert, können vom Anwender, je nach Berechtigung, Rollen zertifiziert werden. Mehr zum Thema Rollen-Zertifizierung finden Sie im Kapitel “5.3.2 Re-/Zertifizierung von Rollen”.

3.2.2 Fehlende Berechtigungen

Wird bei dem zuvor erwähnten Soll-Ist-Vergleich erkannt, dass eine Berechtigungszuweisung nicht existiert, obwohl diese aufgrund des in daccord festgelegten Rollenmodells eigentlich existieren müsste, wird diese unter dem Tab fehlende Berechtigungen angezeigt.

Hinweis: *Lassen Sie sich alle fehlenden Berechtigungen der aktuell angemeldeten Person als Report im PDF-Format ausgeben. Klicken Sie dazu auf das PDF-Icon „Report der fehlenden Berechtigungen" rechts oberhalb der Tabelle mit den fehlenden Berechtigungen.*

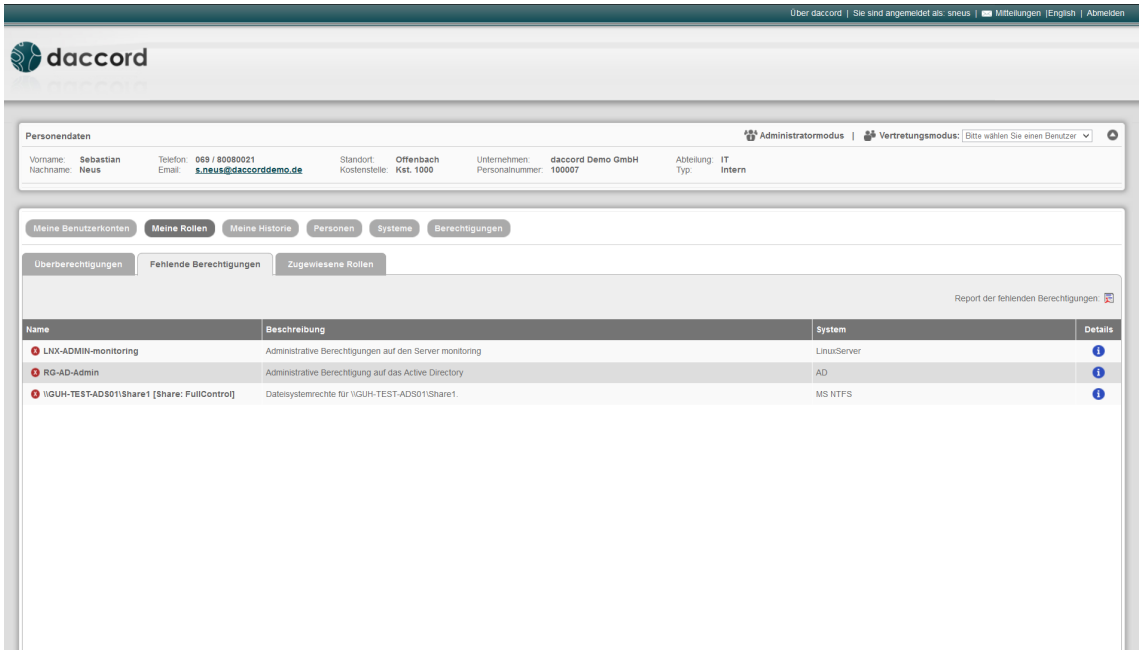


Abbildung 11: Diese Ansicht zeigt alle fehlenden Berechtigungen

Weitere Informationen zu den einzelnen Berechtigungszuweisungen gibt es beim Klick auf das blaue Icon in der Spalte Details. Es öffnet sich ein neues Fenster, indem weitere Informationen zu diesen Eintrag angezeigt werden. Die Informationen sind aufgeteilt auf die Tabs „Allgemein" und „Attribute".

3.2.3 Zugewiesene Rollen

In dem Tab „Zugewiesenen Rollen", werden alle Rollen und dessen verknüpfte Berechtigungen des aktuell angemeldeten Benutzers angezeigt.

Hinweis: *In der Spalte Zuweisungen können Sie erkennen, wieviele Berechtigungen einer Rolle zugewiesen sind. Um die Berechtigungszuweisungen der einzelnen Rollen ein oder aus zu klappen, klicken Sie auf den grauen Pfeil, bei dem entsprechenden Rollen-Eintrag.*

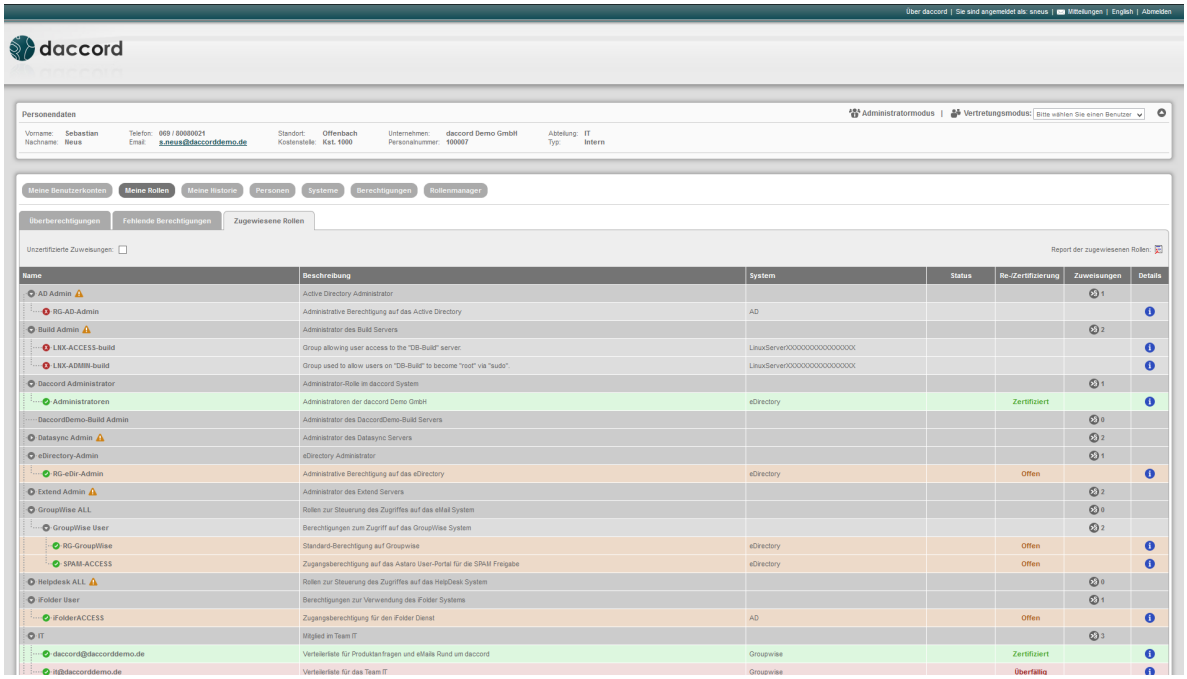


Abbildung 12: Diese Ansicht zeigt alle Rollen und deren zugewiesenen Berechtigungen

Hinweis: *Lassen Sie sich alle „Zugewiesene Rollen" der aktuell angemeldeten Person als Report im PDF-Format ausgeben. Klicken Sie dazu auf das PDF-Icon Report der „Zugewiesene Rollen" rechts oberhalb der Tabelle.*

Je nachdem ob die importierte Berechtigungszuweisung mit dem von daccord vorgegebenen Rollenmodell überein stimmt oder nicht, werden vor dem Eintrag verschiedene Symbole angezeigt. In der folgenden Tabelle werden die Symbole kurz erklärt:

Farbe	Beschreibung
Grün	Berechtigung erhalten und conform mit dem Rollenmodell
Rot	Berechtigung nicht erhalten
Gelb	Recht über zwei Rollen oder zwei Benutzerkonten erhalten

Tabelle 3: Status-Übersicht der zugewiesenen Berechtigungen

Hinweis: *Wird neben einem Rollennamen ein oranges Ausrufezeichen angezeigt, bedeutet dies, dass ein oder mehrere darunter liegende Rechte mit fehlenden Zuweisungen zugeordnet sind. Um sich die fehlerhaften Rechte anzeigen zu lassen, klicken Sie auf den Pfeil ganz links.*

Weitere Informationen zu den einzelnen Berechtigungszuweisungen gibt es beim Klick auf das blaue Icon in der Spalte Details. Es öffnet sich ein neues Fenster, indem weitere Informationen zu diesen Eintrag angezeigt werden.

Die Informationen sind aufgeteilt auf die Tabs „Allgemein", „Attribute" und „Historie". Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

Ist die Re-/Zertifizierung aktiviert, können je nach Berechtigung, die einzelnen Rollen re-/zertifiziert werden. Mehr zum Thema Re-/Zertifizierung finden Sie im Kapitel "5.3.2. Re-/Zertifizierung von Rollen".

3.3 Meine Historie

Das Tab „Meine Historie" bietet dem aktuell angemeldeten Benutzer eine Übersicht über alle, seine Person betreffenden, historischen Daten. Zur besseren Übersicht wurden die historischen Daten in die Tabs „Mich betreffend"„,Initiiert", „Involviert" unterteilt.

Hinweis: *Bitte beachten Sie, dass dieses Tab nur angezeigt wird wenn dies entsprechend konfiguriert ist. Bei Problemen wenden Sie sich bitte an Ihren daccord Systemadministrator.*

Die Ergebnisse lassen sich anhand von folgenden Suchkriterien filtern. Durch das Setzen eines Hackens bei "Erweiterte Suchobtionen anzeigen", werden weitere Suchoptionen angezeigt.

Parameter	Beschreibung
Startdatum	Filtert nach Aktionen, die ab dem angegebenen Datum gestellt wurden.
Enddatum	Filtert nach Aktionen, die bis zum angegebenen Datum gestellt wurden.
Kategorie	Wählen Sie zwischen den Kategorien... • Alle • Person • Benutzerkonto • Berechtigung • Zuweisung um die Suche einzugrenzen.
Aktion	Wählen Sie zwischen den Aktionen... • Alle • Erstellung • Löschen • Klärung • Änderung • Re-/Zertifizierung um die Suche einzugrenzen.

Parameter	Beschreibung
Typ	Wählen Sie zwischen den Typen... • Alle • Systemereignis • Prozess um die Suche einzugrenzen.
Zielobjekt	Geben Sie ein Zielobjekt ein, nach dem gefiltert werden soll.
System	Geben Sie das System des Prozesses ein, nachdem gefiltert werden soll.
Initiator	Geben Sie einen Initiator des Prozesses ein, nachdem gefiltert werden soll.
Ergebnisse	Geben Sie an, wie viele Ergebnisse die Suche zurückliefern soll. Der Standartwert hierfür ist 200.
Antragsname	Geben Sie einen Antragsnamen ein, nachdem gefiltert werden soll.
Unteranträge suchen	Setzen Sie den Hacken, um auch in Unteranträgen zu suchen.

Tabelle 4: Filter für alle Untertabs von „Meine Historie"

In der letzten Spalte „Details" wird je nachdem, wie das daccord User Frontend eingerichtet ist, ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon lassen sich weitere Informationen zu dem ausgewählten Eintrag anzeigen. Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

3.3.1 „Mich betreffend"

In dem Tab „Mich betreffend" werden alle historischen Daten, die das eigene Benutzerkonto betreffen, angezeigt. Die Einträge sind nach Datum sortiert, wobei das aktuellste Datum am Anfang steht. Die Ergebnisse können wie zuvor erwähnt, durch die Angabe von verschiedenen Suchkriterien gefiltert werden.

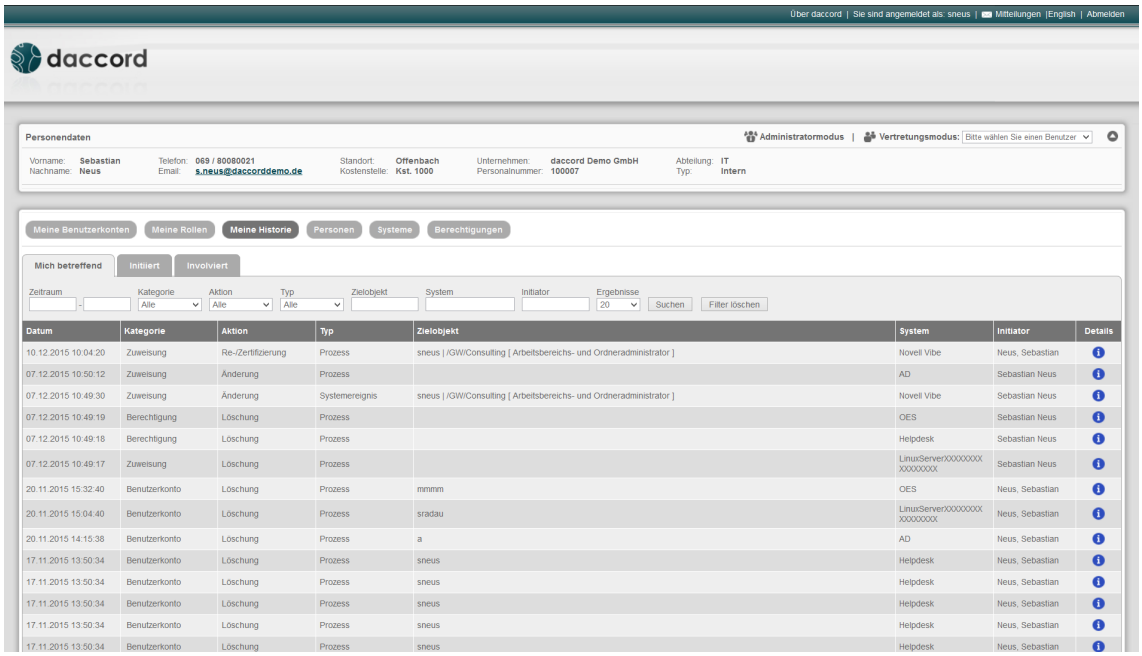


Abbildung 13: Übersicht aller Aktionen die den aktuell angemeldeten Benutzer betreffen

3.3.2 „Initiiert“

In dem Tab „Initiiert” werden alle historischen Aktionen aufgeführt, die von dem aktuell angemeldetem Benutzer ausgelöst wurden. Die Einträge sind nach Datum sortiert, wobei das aktuellste Datum am Anfang steht. Die Ergebnisse können wie zuvor erwähnt, durch die Angabe von verschiedenen Suchkriterien gefiltert werden.

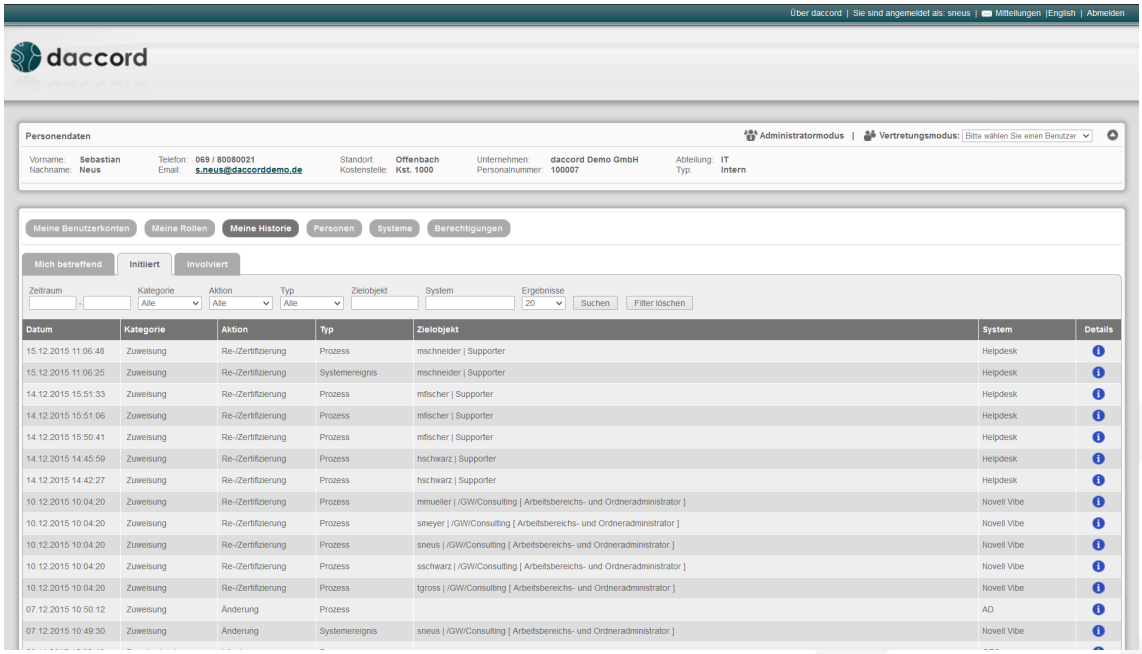


Abbildung 14: Übersicht aller Aktionen die von dem aktuell angemeldeten Benutzer initiiert wurden

3.3.3 „Involviert“

Alle Aktionen, bei denen der aktuell angemeldete Benutzer als Genehmiger involviert ist, werden im Tab „Involviert” angezeigt. Die Einträge sind nach Datum sortiert, wobei das aktuellste Datum am Anfang steht. Die Ergebnisse können wie zuvor erwähnt, durch die Angabe von verschiedenen Suchkriterien gefiltert werden.

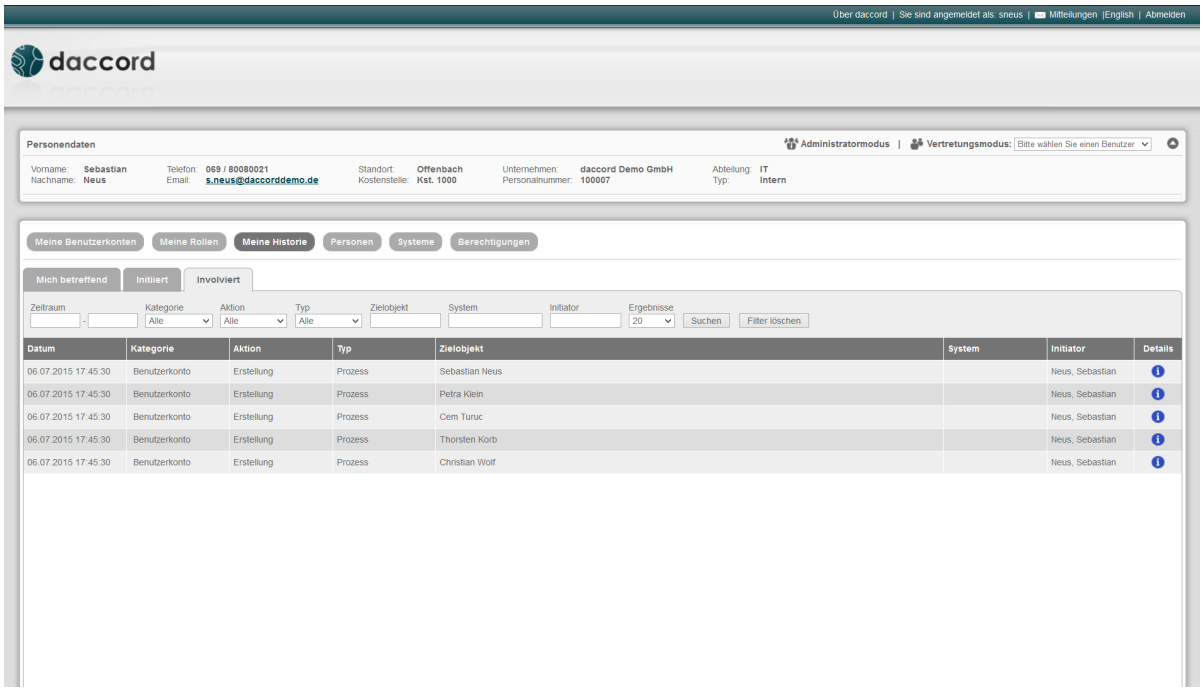


Abbildung 15: Übersicht aller Aktionen bei denen der aktuell angemeldete Benutzer involviert war

3.4 Personen

Im Tab „Personen" finden Sie eine Auflistung aller Personen, für die die angemeldete Person verantwortlich ist. Ist eine Person für eine oder mehrere Personen verantwortlich, wird dieser als „Person Manager" (Personenverantwortlicher) bezeichnet.

Die Anzeige innerhalb dieses Tabs stellt demnach z.B. die Möglichkeit zur Verfügung, für Personalverantwortliche eine Darstellung der Benutzerkonten und Berechtigungen der jeweiligen Mitarbeiter anzubieten.

Hinweis: *Bitte beachten Sie, dass dieses Tab nur angezeigt wird insofern die angemeldete Person für andere Personen als „Person Manager" definiert wurde. Bei Problemen wenden Sie sich bitte an Ihren daccord Systemadministrator.*

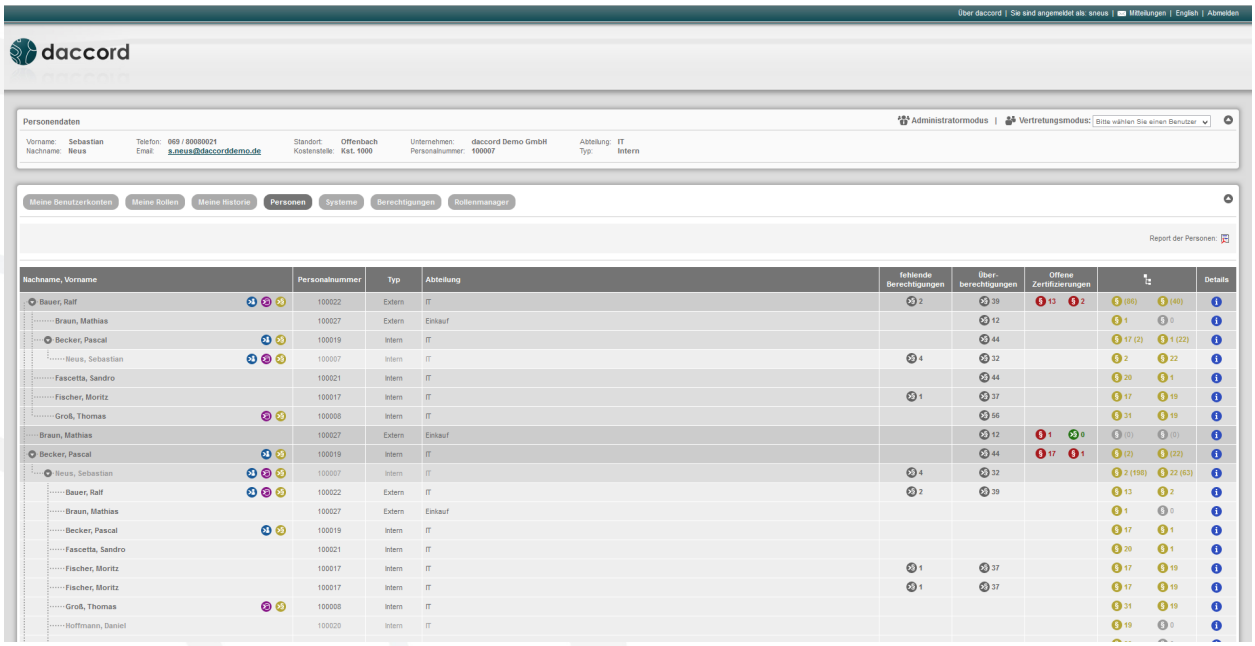


Abbildung 16: Übersicht der Personen

Die Anzahl der Spalten in Ihrer Ansicht, kann leicht abweichen, je nachdem welche Berechtigung Sie haben und ob die Rollen-Zertifizierung aktiviert ist. Eine Auflistung an Spalten und deren Erklärung, finden Sie auf der nachfolgenden Seite.

In der letzten Spalte „Details" wird je nachdem, wie das daccord User Frontend eingerichtet ist, ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon lassen sich weitere Informationen zu dem ausgewählten Eintrag anzeigen. Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

Die einzelnen Spalten der Ansicht „Personen" werden in der folgenden Tabelle kurz erklärt.

Parameter	Beschreibung
Nachname, Vorname	Gibt Name und Vorname der Person an.
Personalnummer	Gibt die Personalnummer der jeweiligen Person an.
Typ	Gibt an ob des sich bei dieser Person um einen Internen oder einen Externen Mitarbeiter handelt.
Abteilung	Gibt die Abteilung an, in der diese Person arbeitet.
fehlende Berechtigungen	Anzahl der fehlenden Berechtigungen werden angezeigt.
Überberechtigungen	Anzahl der vorhandenen Überberechtigungen werden angezeigt.
Offene Zertifizierungen	Vorhandene Überberechtigungen werden in dieser Spalte angezeigt. Ist die Rollen-Zertifizierung aktiv, werden die offenen Zertifizierungen in "Überberechtigungen" und "Rollen-Zuweisungen" unterteilt. Es wird jeweils die Anzahl der noch zu Zertifizierenden Berechtigungen und Rollen angezeigt.
Untergeordnete Zertifizierungen	Ist ein Person-Manager angemeldet, werden ihm in dieser Spalte die Anzahl noch zu zertifizierenden Berechtigungen angezeigt, die vom untergeordneten Personen-Manager noch zertifiziert werden müssen.
Details	Erlaubt das Öffnen der Details einer Person.

Tabelle 5: Tabelle der Übersichtsseite „Personen"

Hinweis: *Falls Sie nicht genau wissen, wofür welche Zahl in dieser Ansicht steht, können Sie mit der Maus über das Symbol oder die Anzahl gehen, und erhalten einen Titel mit einer ausführlichen Beschreibung angezeigt.*

Es gibt insgesamt vier verschiedene Manager-Typen. Diese sind der „Person Manager", „Right Manager" „System Manager"und „Role Manager". Die Aufgaben der in dieser Ansicht benötigten Manager werden in der folgenden Tabelle erklärt:

Managerart	Beschreibung
„Person Manager" (blaue Symbol)	Der „Person Manager" ist verantwortlich für einen bestimmten Personenkreis. Er kann z.B. die Löschung eines Benutzerkontos oder einer Berechtigungszuweisung, einer Person die ihm zugewiesen ist, beantragen.
„Right Manager" (grüne Symbol)	Ist verantwortlich für kritische Berechtigungen (z.B. spezielle Adminberechtigungen) die speziell überwacht werden müssen.
„Role Manager"	Ist verantwortlich für das Rollen-Modell. Er kann einzelne oder alle Rollen des Rollen-Modells re-/zertifizieren.
„System Manager" (lila Symbol)	Der „System Manager" ist für alle Benutzerkonten, Berechtigungen und Berechtigungszuweisungen eines Systems verantwortlich.

Tabelle 6: Tabelle der Managerarten

Ist die aktuell angemeldete Person ein „Person Manager" ist dieser für die ihm zugewiesenen Personen verantwortlich. In der Spalte "Offene Re-/Zertifizierungen" werden ihm die Rechte und ggf. Rollen angezeigt, die er bei der jeweiligen Person noch zu re-/zertifizieren hat. Sofern die Re-/Zertifizierung aktiviert ist, werden in der Spalte rechts daneben, die Re-/Zertifizierungen angezeigt, die von den untergeordneten Personen-Managern noch zu re-/zertifizieren sind.

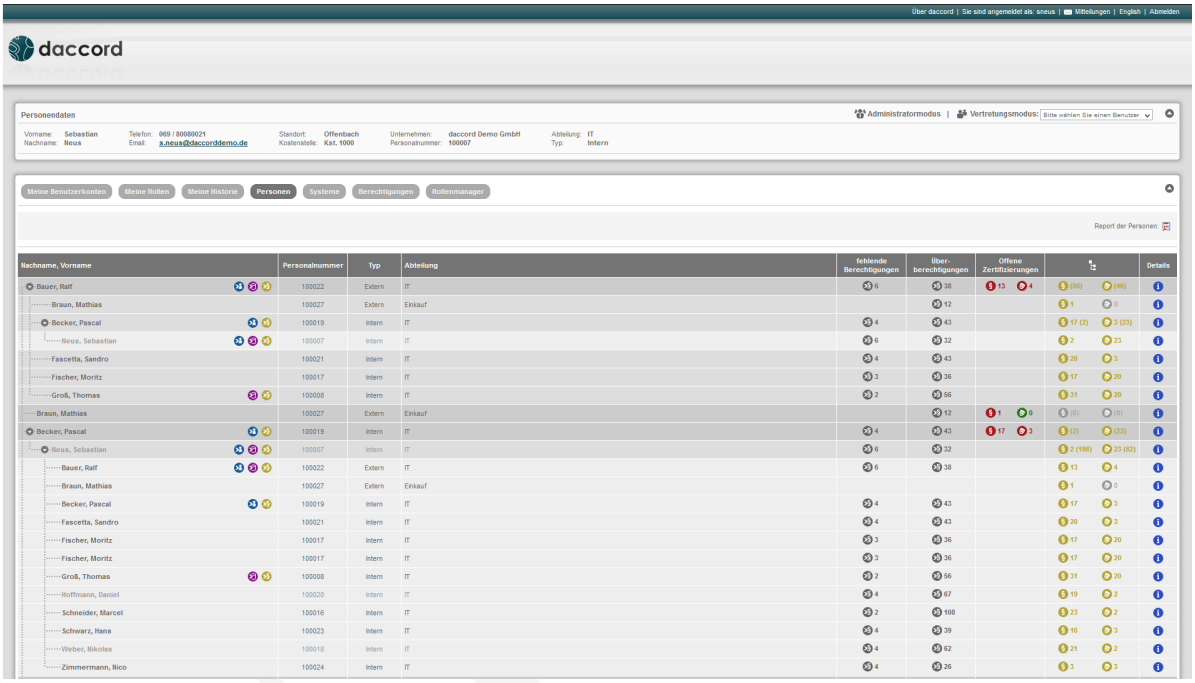


Abbildung 17: Status-Anzeige der Re-/Zertifizierungen eines „Person Manager"

3.4.1 Dokumentation der Details

Über das blaue Info-Icon haben Sie die Möglichkeit, Details zu einer Person aufzurufen. Es werden alle Benutzerkonten, Berechtigungen, Rollen und historische Daten des ausgewählten Benutzers angezeigt.

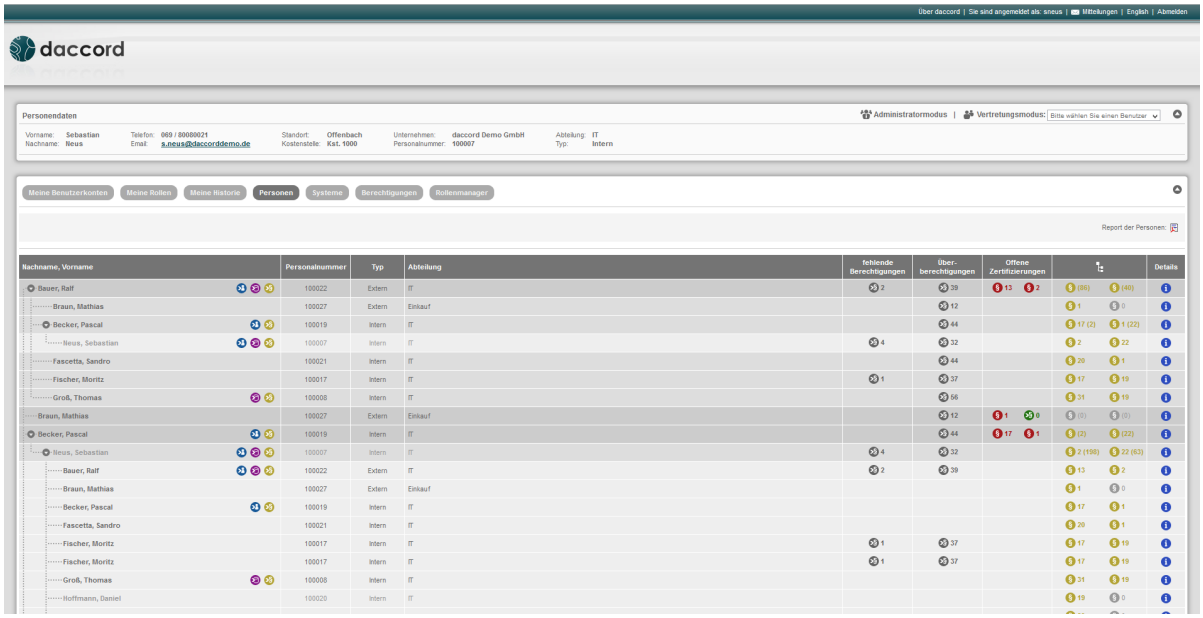


Abbildung 18: Übersicht der Personen

Es wird ein neues Tab im Browser geöffnet, daher können mehrere Personen Details gleichzeitig aufgerufen und verglichen werden.

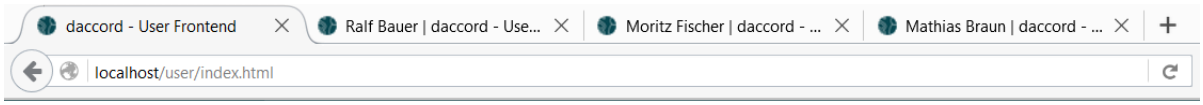


Abbildung 19: Mehrere Benutzer Details sind geöffnet und können verglichen werden

Im oberen Bereich werden die Personendaten des ausgewählten Benutzers aufgeführt. Eine ausführliche Auflistung und Beschreibung der Personendaten finden Sie im Kapitel „4. daccord User Frontend Personendaten".

Unter den Personendaten, befinden sich je nach Einstellung des daccord User Frontends die Tabs „Benutzerkonten", „Rollen", sowie „Historie". Die Ansichten und Funktionen sind die selben wie die bereits erklärten Tabs „Meine Benutzerkonten" (siehe 7.1), „Meine Rollen" (siehe 7.2), „Meine Historie" (siehe 7.3). Allerdings beziehen sich die angezeigten Informationen nicht auf den aktuell angemeldeten Benutzer sondern auf den ausgewählten Benutzer.

Hinweis: *Um einen Report über alle Benutzerkonten der ausgewählten Person zu ziehen, klicken Sie oben rechts oberhalb der Auflistung auf „Report der Benutzerkonten". Darauf hin wird eine PDF generiert und zum Download angeboten.*

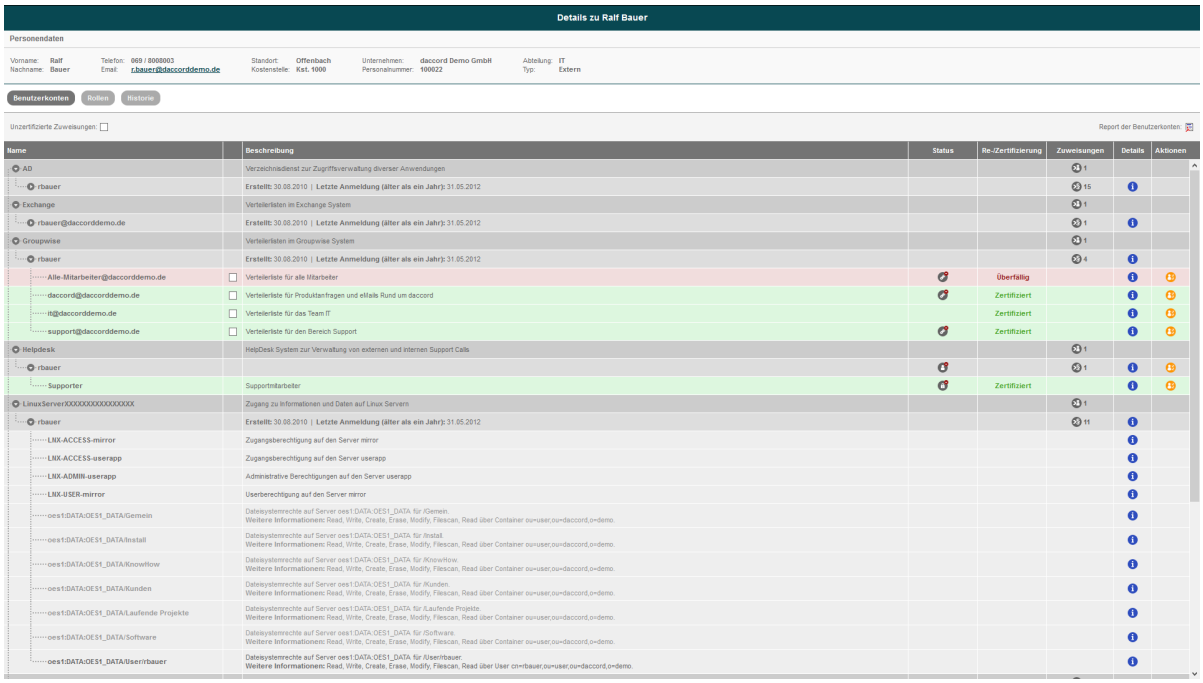


Abbildung 20: Details zu einer ausgewählten Personen im Tab „Benutzerkonto"

3.5 Systeme

Das Tab „Systeme" beinhaltet alle Benutzerkonten und Berechtigungen auf die Systeme, für die die aktuell angemeldete Person „System Manager" ist. Für eine bessere Übersicht, wurden die Informationen zu den Benutzerkonten und Berechtigungen in zwei Tabs aufgeteilt.

Hinweis: *Bitte beachten Sie, dass das „Systeme"-Tab nur angezeigt wird insofern die angemeldete Person als „System Manager" definiert wurde. Bei Problemen wenden Sie sich bitte an Ihren daccord Systemadministrator.*

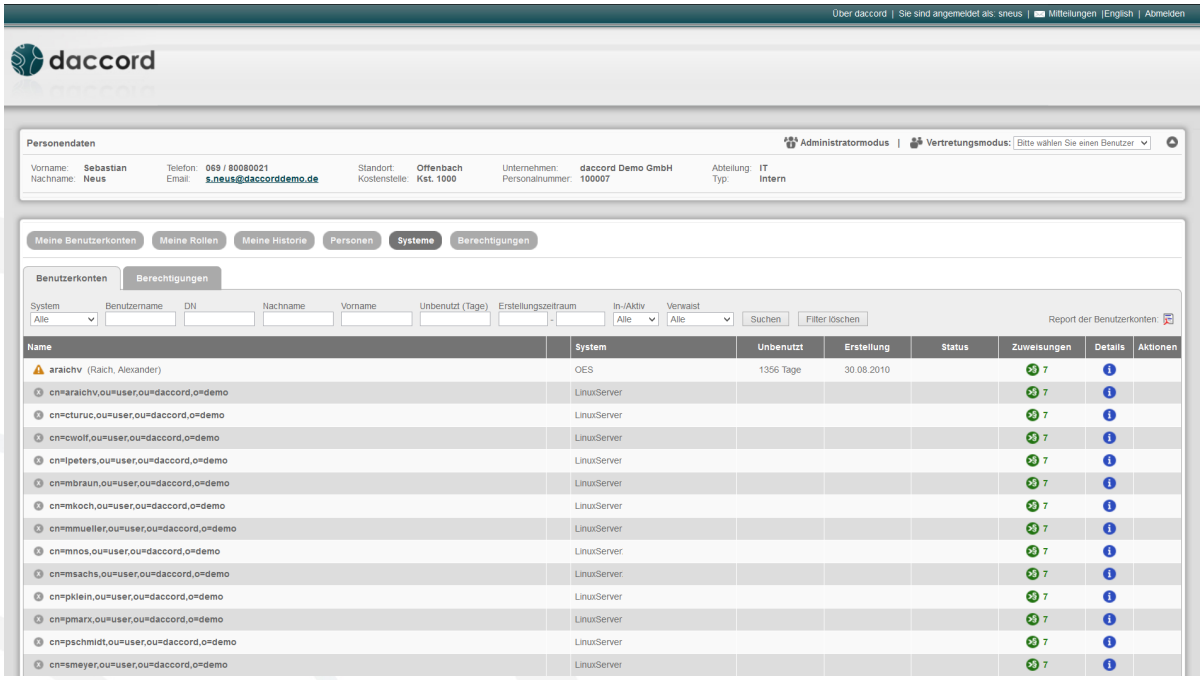


Abbildung 21: Sichtweise: Benutzerkonten im Tab Systeme

In der letzten Spalte „Details" wird je nachdem, wie das daccord User Frontend eingerichtet ist, ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon lassen sich weitere Informationen zu dem ausgewählten Eintrag anzeigen. Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

3.5.1 Sichtweise „Benutzerkonten"

Das Subtab „Benutzerkonten" bietet Ihnen die Möglichkeit, die Benutzerkonten der einzelnen Systeme anzeigen zu lassen. Die Benutzerkonten lassen sich über die Filterfunktion filtern. Die Darstellung weicht dabei von der alternativen Darstellung „Berechtigungen" ab.

Parameter	Beschreibung
Benutzername	Zeigt den Namen des Benutzerkontos an. Die Symbole vor den Benutzernamen zeigen deren Status an. • Grünes Symbol für aktive Benutzerkonten, die einer Person zugeordnet sind. • Rotes Symbol für aktive Benutzerkonten, die keiner Person zugeordnet sind. • Graues Symbol für inaktive Benutzerkonten.
System	Name des Systems, zu dem das Benutzerkonto gehört.
Unbenutzt	Zeigt an, wie viel Zeit (in Tagen) seit der letzten Benutzung des Benutzerkontos vergangen ist.
Erstellung	Zeigt das Datum an, an dem das Benutzerkonto erstellt wurde.
Status	Wurde für dieses Benutzerkonto eine Aktion angestoßen (z.B. Löschen) und befindet sich diese noch in der Bearbeitung, wird an dieser Stelle ein entsprechendes Icon angezeigt.
Zuweisungen	Zeigt an, wieviele Berechtigungen das Benutzerkonto auf das jeweilige System hat.
Details	Erlaubt das Öffnen der Details eines Benutzerkontos.
Aktionen	Sofern für ein Benutzerkonto eine Aktion möglich ist, kann diese über das orange „Aktion"-Icon angestoßen werden. Folgende Aktionen sind möglich: • Löschen - Die hinterlegte Aktion zum Löschen eines Benutzerkontos wird ausgeführt • Klären - Die hinterlegte Aktion zum Klären eines Benutzerkontos wird ausgeführt • Re-/Zertifizierung - Die hinterlegte Aktion zum Re-/Zertifizierung eines Benutzerkontos wird ausgeführt

Tabelle 7: Sichtweise der Benutzerkonten

Hinweis: *Um einen Report über alle Benutzerkonten der angebundenen Systeme zu ziehen, klicken Sie oben rechts oberhalb der Auflistung auf „Report der Benutzerkonten". Darauf hin wird eine PDF generiert und zum Download angeboten.*

3.5.1.1 Dokumentation der Filtermöglichkeiten

Die Einträge in der Liste können nach verschiedenen Kriterien gefiltert werden. In der folgenden Tabelle, werden die Kriterien des Filters aufgeführt und kurz erläutert.

Parameter	Beschreibung
System	Wählen Sie ein System aus, dessen Benutzerkonten Sie einsehen möchten.
Benutzername	Geben Sie an, für welchen Benutzer Sie die Benutzerkonten angezeigt bekommen möchten.
DN	Geben Sie den Distinguished Namen des Benutzers an, den Sie angezeigt bekommen möchten.
Nachname	Geben Sie als Filter den Nachnamen eines Benutzers an, dessen Benutzerkonten Sie angezeigt bekommen möchten.
Vorname	Geben Sie als Filter den Vornamen eines Benutzers an, dessen Benutzerkonten Sie angezeigt bekommen möchten.
Unbenutzt (Tage)	Geben Sie an, wieviele Tage das Benutzerkonto mindestens ungenutzt sein muss, um es anzuzeigen.
Startdatum	Filtert nach Benutzerkonten, die ab dem angegebenen Datum erstellt wurden.
Enddatum	Filtert nach Benutzerkonten, die bis zum angegebenen Datum erstellt wurden.
In-/Aktiv	Wählen Sie den Status der Benutzerkonten. Mögliche Varianten sind • Alle • Aktive - Aktive Benutzerkonten • Inaktive - Inaktive Benutzerkonten Systeme.
Verweist	Wählen Sie, ob die Benutzerkonten einer Person zugeordnet sind. Filtern nach • Alle • Einer Person zugewiesen • Keiner Person zugewiesen ist möglich.

Tabelle 8: Filter der Sichtweise „Benutzerkonten"

3.5.1.2 Erklärung „Zuweisungen"

In der Sichtweise „Benutzerkonten" können die Berechtigungszuweisungen eines Benutzerkontos ausgewertet werden. Die Anzahl der jeweiligen Zuweisungen wird in der Spalte „Zuweisungen" angezeigt. Neben der Anzahl der Zuweisungen befindet sich ein grünes Icon. Mit einem Klick auf dieses Icon, werden die Zuweisungen aufgelistet.

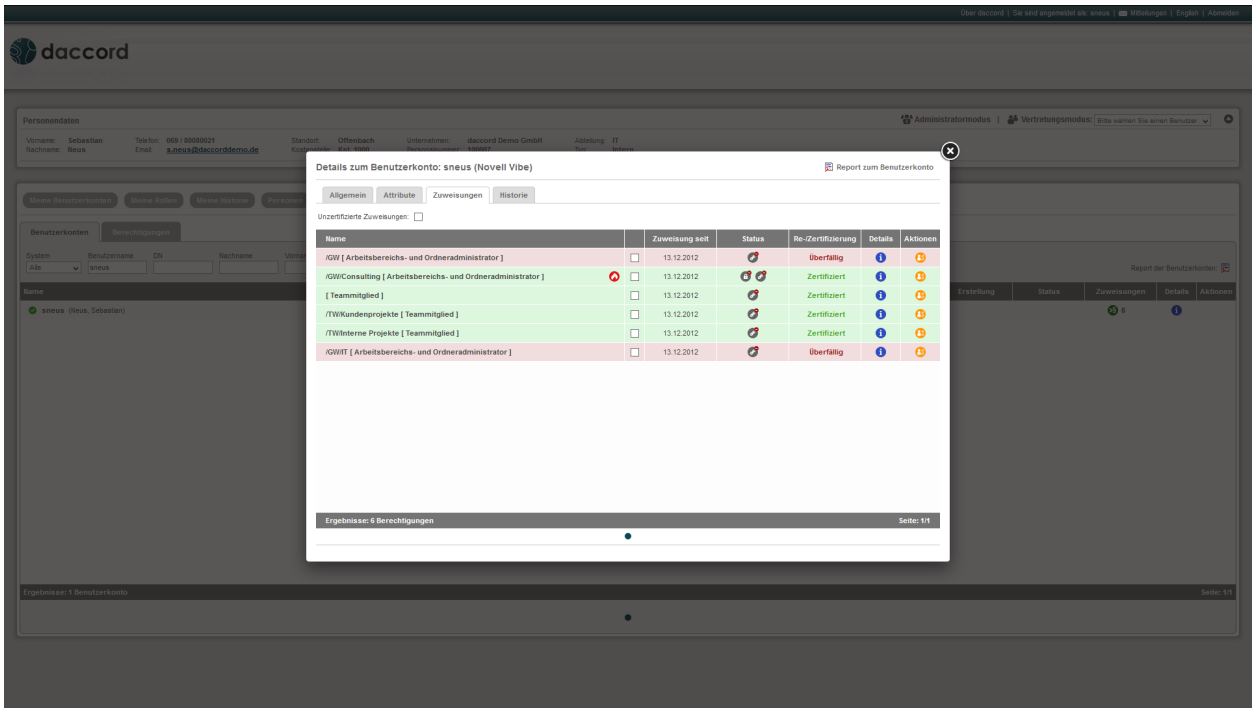


Abbildung 22: Auflistung der zugewiesenen Berechtigungen zu einem Benutzerkonto

Hinweis: *Um einen Report über alle Berechtigungen des ausgewählten Benutzerkontos zu ziehen, klicken Sie oben rechts oberhalb der Auflistung auf „Report zum Benutzerkonto". Darauf hin wird eine PDF generiert und zum Download angeboten.*

Ist die Re-/Zertifizierung aktiviert, können je nach Berechtigung, die einzelnen Zuweisungen re-/zertifiziert werden. Mehr zum Thema Re-/Zertifizierung finden Sie im Kapitel "5.3.1. Re-/Zertifizierung von Rollen".

In der folgenden Tabelle werden die einzelnen Spalten der Ansicht „Zuweisungen" kurz erklärt.

Parameter	Beschreibung
Name	Zeigt den Namen der Zuweisung an.
Zuweisung seit	Gibt an, seit wann die Berechtigung dem Benutzerkonto zugewiesen ist,
Status	Wurde für diese Berechtigung eine Aktion angestoßen (z.B. Löschen) und befindet sich diese noch in der Bearbeitung, wird an dieser Stelle ein entsprechendes Icon angezeigt.
Re-/Zertifizierung	Wird für diese Berechtigung eine Re-/Zertifizierung benötigt, wird in dieser Spalte der Status der Re-/Zertifizierung angezeigt. Folgende Werte sind möglich: • Offen - Es wurde noch keine Re-/Zertifizierung durch geführt, obwohl sie benötigt wird. • Überfällig - Die Gültigkeit der Re-/Zertifizierung ist abgelaufen. Die Berechtigung muss vom Vorgesetzten erneut bestätigt werden. • Re-/Zertifiziert - Die Berechtigung ist erfolgreich Re-/Zertifiziert und noch gültig.
Details	Erlaubt das Öffnen der Details einer Berechtigung.
Aktionen	Sofern für ein Berechtigung eine Aktion möglich ist, kann diese über das orange „Aktion"-Icon angestoßen werden. Folgende Aktionen sind möglich: • Löschen - Die hinterlegte Aktion zum Löschen einer Berechtigung wird ausgeführt • Klären - Die hinterlegte Aktion zum Klären einer Berechtigung wird ausgeführt • Re-/Zertifizierung - Die hinterlegte Aktion zum Re-/Zertifizierung einer berechtigung wird ausgeführt

Tabelle 9: Übersicht der Zuweisungen

3.5.2 Sichtweise „Berechtigungen”

Das Tab „Berechtigungen” bietet Ihnen die Möglichkeit, alle Berechtigungen der Systeme anzeigen zu lassen, für die die aktuell angemeldete Person „System Manager” ist. Die Darstellung weicht dabei von der alternativen Darstellung „Benutzerkonten” ab.

Hinweis: *Um einen Report über alle Berechtigungen der angebundenen Systeme zu ziehen, klicken Sie oben rechts oberhalb der Auflistung auf „Report der Berechtigungen”. Darauf hin wird eine PDF generiert und zum Download angeboten.*

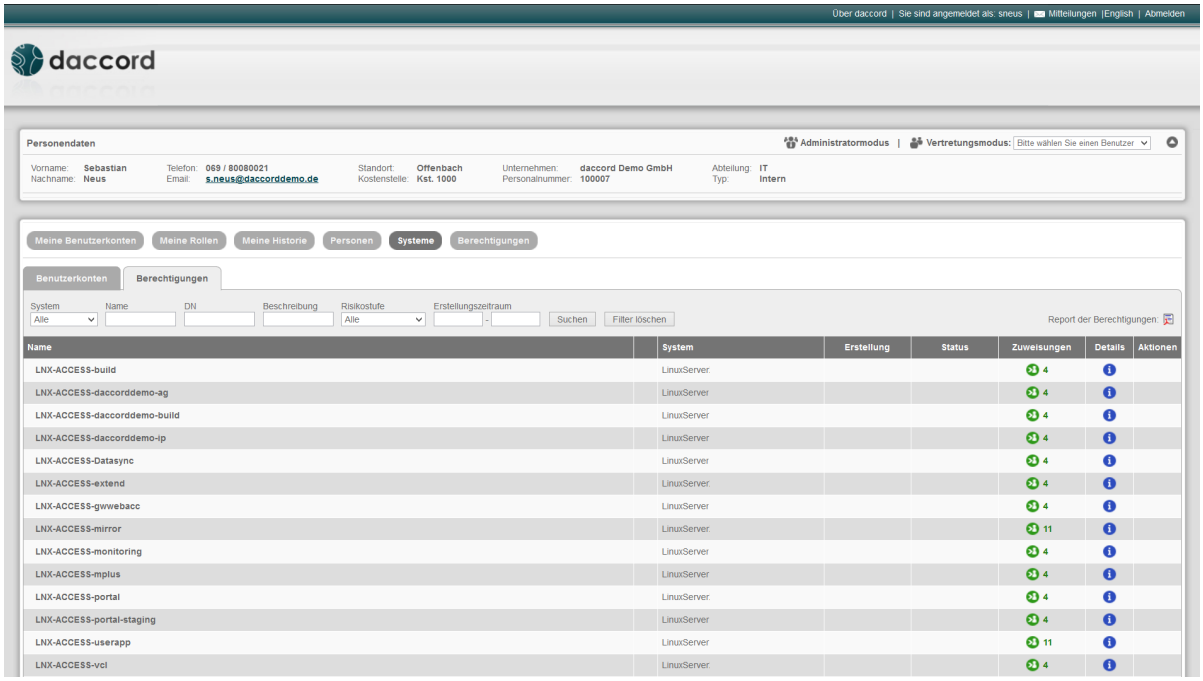


Abbildung 23: Sichtweise „Berechtigungen” im Tab Systeme

Parameter	Beschreibung
Name	Zeigt den Namen der Berechtigung an.
System	Name des Systems, zu dem die Berechtigung gehört.
Erstellung	Zeigt das Datum an, an dem die Berechtigung erstellt wurde.
Status	Wurde für diese Berechtigung eine Aktion angestoßen (z.B. Löschen) und befindet sich diese noch in der Bearbeitung, wird an dieser Stelle ein entsprechendes Icon angezeigt.
Zuweisungen	Zeigt an, wieviele Benutzerkonten der ausgewähltem Berechtigung auf dem jeweiligem System zugewiesen sind.
Details	Erlaubt das Öffnen der Details einer Berechtigung.
Aktionen	Sofern für ein Berechtigung eine Aktion möglich ist, kann diese über das orange „Aktion"-Icon angestoßen werden. Folgende Aktionen sind möglich: • Löschen - Die hinterlegte Aktion zum Löschen einer Berechtigung wird ausgeführt • Klären - Die hinterlegte Aktion zum Klären einer Berechtigung wird ausgeführt • Re-/Zertifizierung - Die hinterlegte Aktion zum Re-/Zertifizierung einer berechtigung wird ausgeführt

Tabelle 10: Tabellenstruktur der Sichtweise „Berechtigungen" im Tab Systeme

3.5.2.1 Dokumentation der Filtermöglichkeiten

Die Einträge in der Liste können nach verschiedenen Kriterien gefiltert werden. In der folgenden Tabelle, werden die Kriterien des Filters aufgeführt und kurz erläutert.

Parameter	Beschreibung
System	Wählen Sie ein System aus, dessen Berechtigungen Sie einsehen möchten.
Name	Geben Sie den Namen der Berechtigung an, nach der Sie filtern wollen.
DN	Geben Sie den Distinguished Namen der Berechtigung an, den Sie angezeigt bekommen möchten.
Beschreibung	Geben Sie die Beschreibung an,nach der Sie filtern wollen.
Risikostufe	Wählen Sie eine bestimmte Risikostufe aus, dessen Berechtigungen angezeigt werden sollen. Mögliche Risikostufen sind • Alle • Niedriges Risiko • Erhöhtes Risiko • Hohes Risiko
Startdatum	Filtert nach Berechtigungen, die ab dem angegebenen Datum erstellt wurden.
Enddatum	Filtert nach Berechtigungen, die bis zum angegebenen Datum erstellt wurden.

Tabelle 11: Filter der Sichtweise Berechtigungen

3.5.2.2 Erklärung „Zuweisungen"

In der Sichtweise „Berechtigungen" können die zu einer Berechtigung zugewiesenen Benutzerkonten ausgewertet werden. Die Anzahl der jeweiligen Zuweisungen wird in der Spalte „Zuweisungen" angezeigt. Neben der Anzahl der Zuweisungen wird ein grünes Icon angezeigt. Mit einem Klick auf dieses Icon, werden die Zuweisungen aufgelistet.

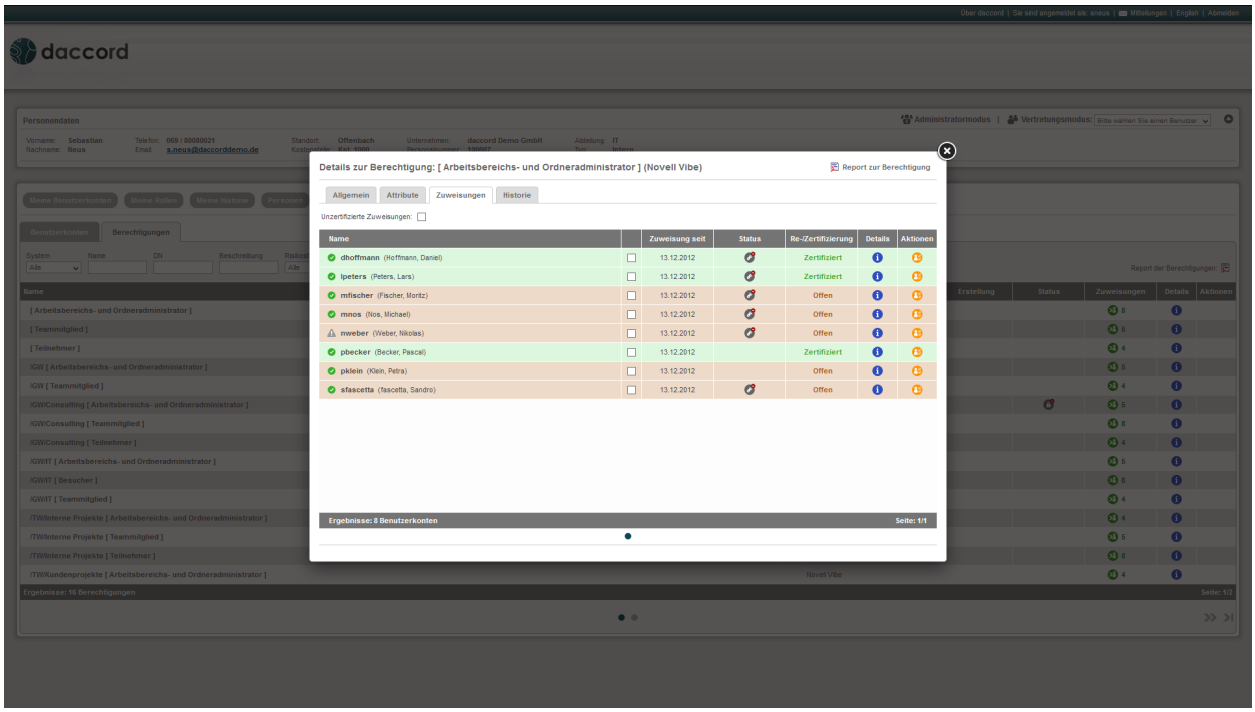


Abbildung 24: Übersicht der Zuweisungen von Benutzerkonten zu einer Berechtigung

Hinweis: *Um einen Report über alle Berechtigungen des ausgewählten Benutzerkontos herunterzuladen, klicken Sie oben rechts oberhalb der Auflistung auf „Report der Berechtigungen". Darauf hin wird eine PDF generiert und zum Download angeboten.*

Ist die Re-/Zertifizierung aktiviert, können je nach Berechtigung, die einzelnen Zuweisungen re-/zertifiziert werden. Mehr zum Thema Re-/Zertifizierung finden Sie im Kapitel "5.3.1. Re-/Zertifizierung von Rollen".

Parameter	Beschreibung
Name	Zeigt den Namen des Benutzerkontos an. Die Symbole vor den Benutzernamen zeigen deren Status an. • Grünes Symbol für aktive Benutzerkonten, die einer Person zugeordnet sind. • Rotes Symbol für aktive Benutzerkonten, die keiner Person zugeordnet sind. • Graues Symbol für inaktive Benutzerkonten.
Zuweisung seit	Gibt an, seit wann das Benutzerkonto der Berechtigung zugewiesen ist.
Status	Wurde für dieses Benutzerkonto eine Aktion angestoßen (z.B. Löschen) und befindet sich diese noch in der Bearbeitung, wird an dieser Stelle ein entsprechendes Icon angezeigt.
Re-/Zertifizierung	Wird für dieses Recht eine Re-/Zertifizierung benötigt, wird in dieser Spalte der Status der Re-/Zertifizierung angezeigt. Folgende Werte sind möglich: • Offen - Es wurde noch keine Re-/Zertifizierung durch geführt, obwohl sie benötigt wird. • Überfällig - Die Gültigkeit der Re-/Zertifizierung ist abgelaufen. Die Berechtigung muss vom Vorgesetzten erneut bestätigt werden. • Re-/Zertifiziert - Die Berechtigung ist erfolgreich Re-/Zertifiziert und noch gültig.
Details	Erlaubt das Öffnen der Details eines Benutzerkontos.
Aktionen	Sofern für ein Benutzerkonto eine Aktion möglich ist, kann diese über das orange „Aktion"-Icon angestoßen werden. Folgende Aktionen sind möglich: • Löschen - Die hinterlegte Aktion zum Löschen eines Benutzerkontos wird ausgeführt • Klären - Die hinterlegte Aktion zum Klären eines Benutzerkontos wird ausgeführt • Re-/Zertifizierung - Die hinterlegte Aktion zum Re-/Zertifizierung eines Benutzerkontos wird ausgeführt

Tabelle 12: Sichtweise Berechtigungen - Ansicht Zuweisungen

3.6 Berechtigungen

Im Tab „Berechtigungen" finden Sie eine Auflistung aller Berechtigungen, die der angemeldeten Person als „Right Manager" (Berechtigungsverantwortlicher) zugewiesen wurden.

Hinweis: *Bitte beachten Sie, dass dieses Tab nur angezeigt wird insofern die angemeldete Person als „Right Manager" definiert wurde. Bei Problemen wenden Sie sich bitte an Ihren daccord Systemadministrator.*

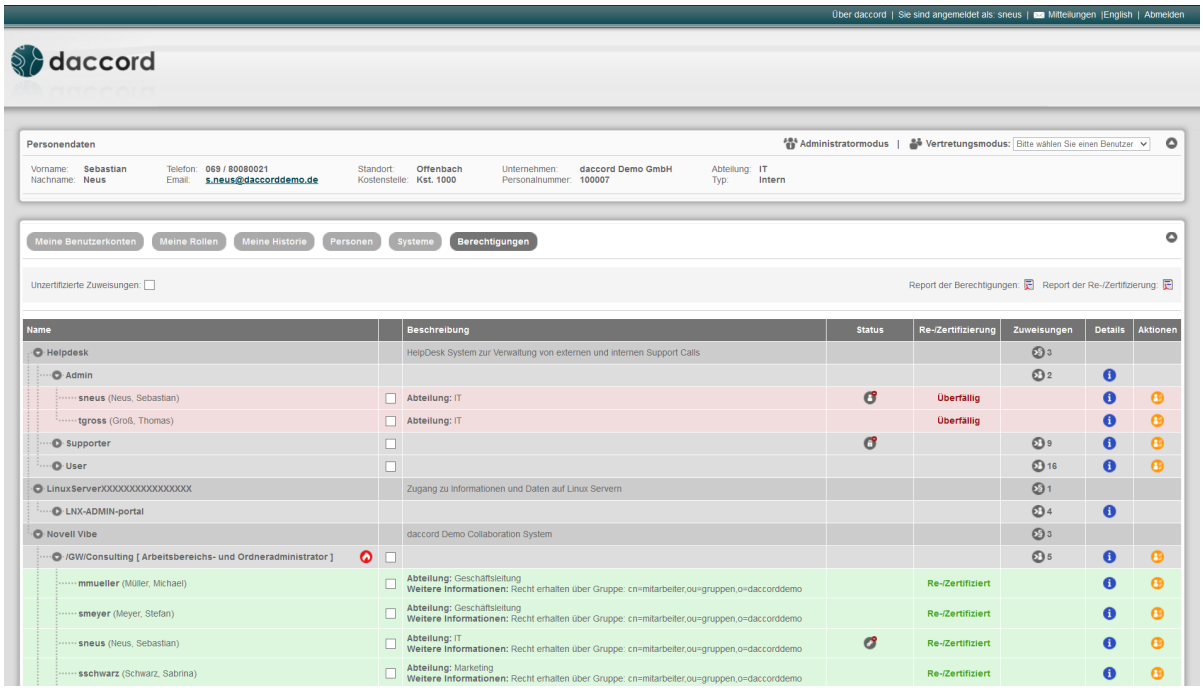


Abbildung 25: Berechtigungen

Die Anzeige der Berechtigungen wird zunächst nach den jeweiligen Systemen sortiert, zu denen die Berechtigungen gehören. Unter den jeweiligen Berechtigungen können die Benutzerkonten eingesehen werden, die die jeweilige Berechtigung besitzen.

Hinweis: *Wenn Sie sich nur unzertifizierte Zuweisungen anzeigen lassen möchten, können Sie dies tun, indem Sie links oben über der Tabelle die Checkbox "Unzertifizierte Zuweisungen" anhacken.*

In dieser Übersicht lassen sich zwei Reporte generieren und als PDF downloaden. Zum einen kann ein Report über alle angezeigten Berechtigungen erstellt werden. Klicken Sie dazu auf das PDF-Icon „Report der Berechtigung". Desweiteren lässt sich ein Report erzeugen in dem nur alle Informationen zu Berechtigungen mit Re-/Zertifizierungen aufgelistet wird. Klicken Sie dazu auf das PDF-Icon „Report der Re-/Zertifizierung".

In der letzten Spalte „Details" wird je nachdem, wie das daccord User Frontend eingerichtet ist, ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon lassen sich weitere Informationen zu dem ausgewählten Eintrag anzeigen. Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

3.6.1 Dokumentation der Tabelle

In der folgenden Liste werden die einzelnen Spalten näher erläutert:

Parameter	Beschreibung
Name	Zeigt den Namen der Berechtigung an.
Beschreibung	Zeigt eine Beschreibung der Berechtigung an.
Status	Wurde für diese Berechtigung eine Aktion angestoßen (z.B. Löschen) und befindet sich diese noch in der Bearbeitung, wird an dieser Stelle ein entsprechendes Icon angezeigt.
Re-/Zertifizierung	Wird für dieses Recht eine Re-/Zertifizierung benötigt, wird in dieser Spalte der Status der Re-/Zertifizierung angezeigt. Folgende Werte sind möglich: • Offen - Es wurde noch keine Re-/Zertifizierung durch geführt, obwohl sie benötigt wird. • Überfällig - Die Gültigkeit der Re-/Zertifizierung ist abgelaufen. Die Berechtigung muss vom Vorgesetzten erneut bestätigt werden. • Re-/Zertifiziert - Die Berechtigung ist erfolgreich Re-/Zertifiziert und noch gültig.
Zuweisungen	Zeigt an, wieviele Benutzerkonten der Berechtigung zugeordnet sind.
Details	Erlaubt das Öffnen der Details einer Berechtigung.
Aktionen	Sofern für ein Berechtigung eine Aktion möglich ist, kann diese über das orange „Aktion"-Icon angestoßen werden. Folgende Aktionen sind möglich: • Löschen - Die hinterlegte Aktion zum Löschen einer Berechtigung wird ausgeführt • Klären - Die hinterlegte Aktion zum Klären einer Berechtigung wird ausgeführt • Re-/Zertifizierung - Die hinterlegte Aktion zum Re-/Zertifizierung einer berechtigung wird ausgeführt

Tabelle 13: Erläuterung der Ansicht „Berechtigungen"

3.7 Rollenmanager

Im Tab „Rollenmanager" finden Sie eine Auflistung aller Rollen, die der angemeldeten Person als „Role Manager" (Rollenverantwortlicher) zugewiesen wurden.

Hinweis: *Bitte beachten Sie, dass dieses Tab nur angezeigt wird insofern die angemeldete Person für Rollen als „Role Manager" definiert wurde. Bei Problemen wenden Sie sich bitte an Ihren daccord Systemadministrator.*

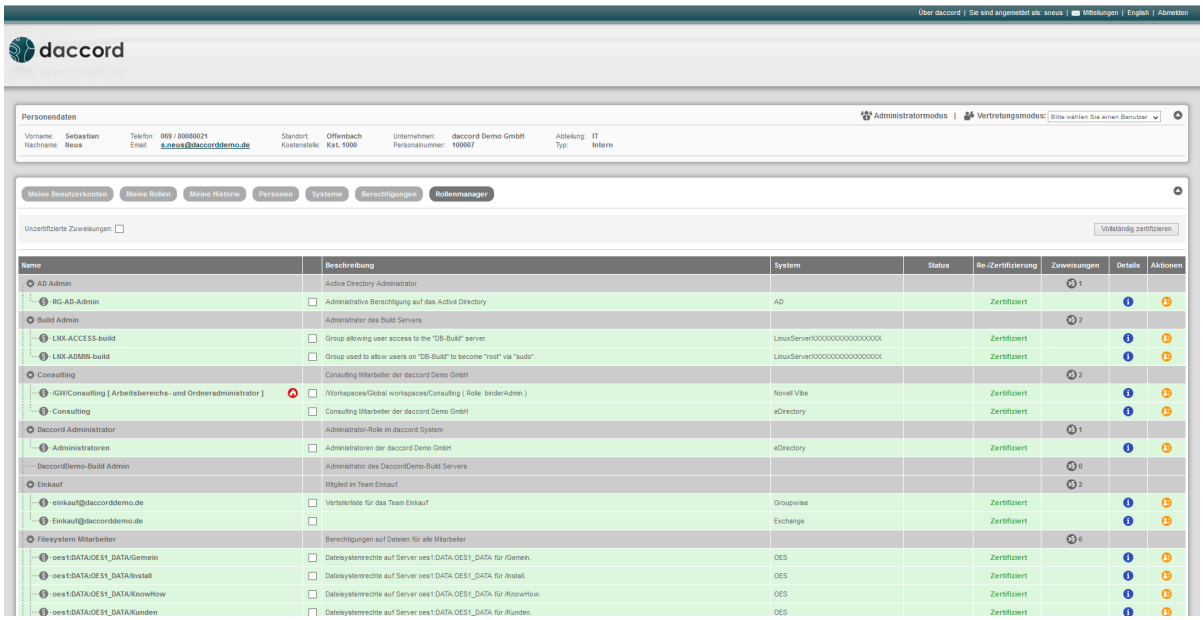


Abbildung 26: Rollenmanager

In der Ansicht 'Rollenmanager' werden alle Rollen angezeigt, die dem Rolemanager zugeordnet sind. In der darunter liegenden Ebene befinden sich die Berechtigungen, die der jeweiligen Rolle zugewiesen sind, sowie ggf. Subrollen. Je nachdem, ob die Rollen-Zertifizierung aktiviert ist, lassen sich die einzelnen Rollen-Zuweisungen re-/zertifizieren.

Hinweis: *Wenn Sie sich nur unzertifizierte Rollen-Zuweisungen anzeigen lassen möchten, können Sie dies tun, indem Sie links oben über der Tabelle die Checkbox "Unzertifizierte Zuweisungen" anhacken.*

In der letzten Spalte „Details" wird je nachdem, wie das daccord User Frontend eingerichtet ist, ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon lassen sich weitere Informationen zu dem ausgewählten Eintrag anzeigen. Mehr zu den „Details" erfahren Sie in Kapitel „4. daccord User Frontend Details".

3.7.1 Erklärung "Vollständig zertifizieren"

Im "Rolemanager" Tab wird oben rechts ein Button "Vollständig zertifizieren" angezeigt. Damit können alle Rollen-Rechte-Zuweisungen in nur einem Schritt re-/zertifiziert werden.

Mit einem Klick auf den Button "Vollständig zertifizieren", öffnet sich eine Lightbox. Dort können Sie, wie bei einer normalen Re-/Zertifizierung (siehe Kapitel 5.3 Re-/Zertifizierung) auch, die benötigten Informationen angeben. Der blaue Hinweistext, weisst noch mal darauf hin, das beim Absenden dieses Formulars alle Rollen-Rechte-Zuweisungen sowie Rollen-Rollen-Zuweisungen (Subrollen) re-/zertifiziert werden.

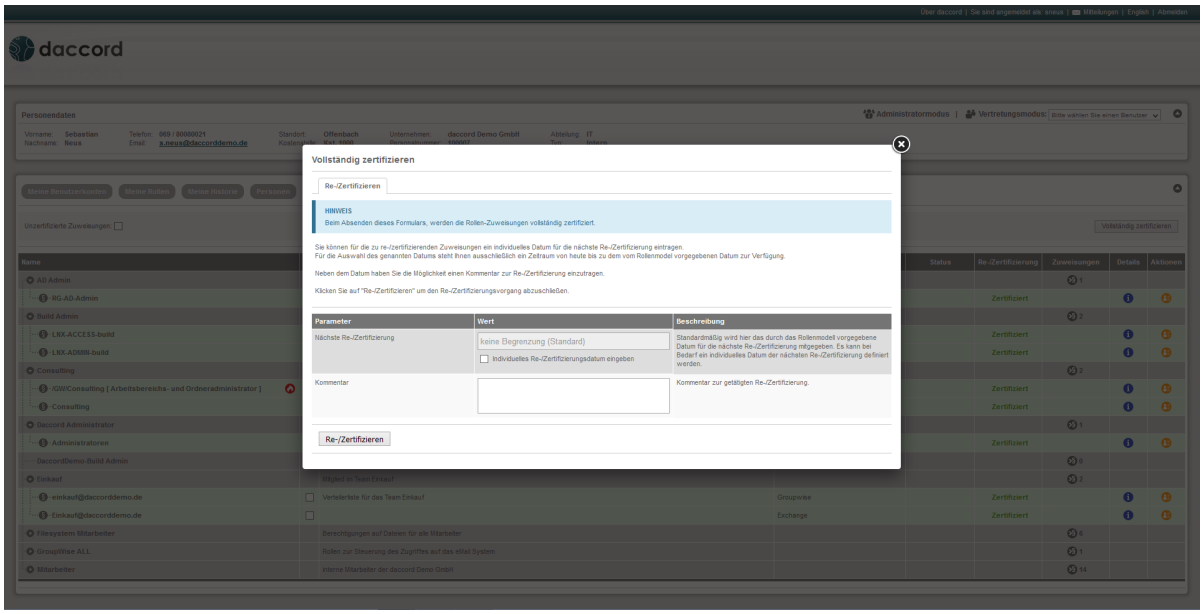


Abbildung 27: Vollständig zertifizieren

Hinweis: *Je nachdem wieviele Rollen-Rechte-Zuweisungen re-/zertifiziert werden, kann der Speichervorgang ein paar Sekunden dauern.*

3.7.2 Dokumentation der Tabelle

In der folgenden Liste werden die einzelnen Spalten näher erläutert:

Parameter	Beschreibung
Name	Zeigt den Namen der Rolle oder der Berechtigung an.
Beschreibung	Zeigt eine Beschreibung der Rolle oder der Berechtigung an.
System	Zeigt an, in welchem System das Recht gilt. Berechtigung an.
Status	Wurde für diese Berechtigung eine Aktion angestoßen (z.B. Löschen) und befindet sich diese noch in der Bearbeitung, wird an dieser Stelle ein entsprechendes Icon angezeigt.
Re-/Zertifizierung	Wird für dieses Recht eine Re-/Zertifizierung benötigt, wird in dieser Spalte der Status der Re-/Zertifizierung angezeigt. Folgende Werte sind möglich: • Offen - Es wurde noch keine Re-/Zertifizierung durch geführt, obwohl sie benötigt wird. • Überfällig - Die Gültigkeit der Re-/Zertifizierung ist abgelaufen. Die Berechtigung muss vom Vorgesetzten erneut bestätigt werden. • Re-/Zertifiziert - Die Berechtigung ist erfolgreich Re-/Zertifiziert und noch gültig.
Zuweisungen	Zeigt an, wieviele Berechtigungen dieser Rolle zugeordnet sind.
Details	Erlaubt das Öffnen der Details einer Berechtigung.
Aktionen	Sofern für ein Berechtigung eine Aktion möglich ist, kann diese über das orange „Aktion"-Icon angestoßen werden. Folgende Aktionen sind möglich: • Löschen - Die hinterlegte Aktion zum Löschen einer Berechtigung wird ausgeführt • Klären - Die hinterlegte Aktion zum Klären einer Berechtigung wird ausgeführt • Re-/Zertifizierung - Die hinterlegte Aktion zum Re-/Zertifizierung einer berechtigung wird ausgeführt

Tabelle 14: Erläuterung der Ansicht „Rollenmanager"

4 daccord User Frontend Details

In den verschieden Ansichten des daccord User Frontend wird in der Spalte „Details" ein blaues Info-Icon angezeigt. Mit einem Klick auf dieses Icon, öffnet sich ein neues Fenster, indem weitere Informationen zu dem ausgewählten Eintrag angezeigt werden. Welche Informationen und Tabs angezeigt werden, hängt zum einen davon ab, wie das daccord User Frontend konfiguriert ist und welcher Eintrag (Benutzerkonto, Berechtigung oder Berechtigungszuweisung) ausgewählt wurde.

Die Tabs „Allgemein", „Zertifizierung", „Attribute", „Zuweisungen" und „Historie" werden in den nächsten Kapiteln näher erläutert.

4.1 Allgemein

Unter dem „Allgemein"-Tab werden die entsprechenden allgemeinen Informationen zur Benutzung, Berechtigung, dem Benutzerkonto und der Person aufgeführt.

Hinweis: *Um einen Report über das ausgewählte Benutzerkonten zu ziehen, klicken Sie oben rechts auf „Report zum Benutzerkonto".*

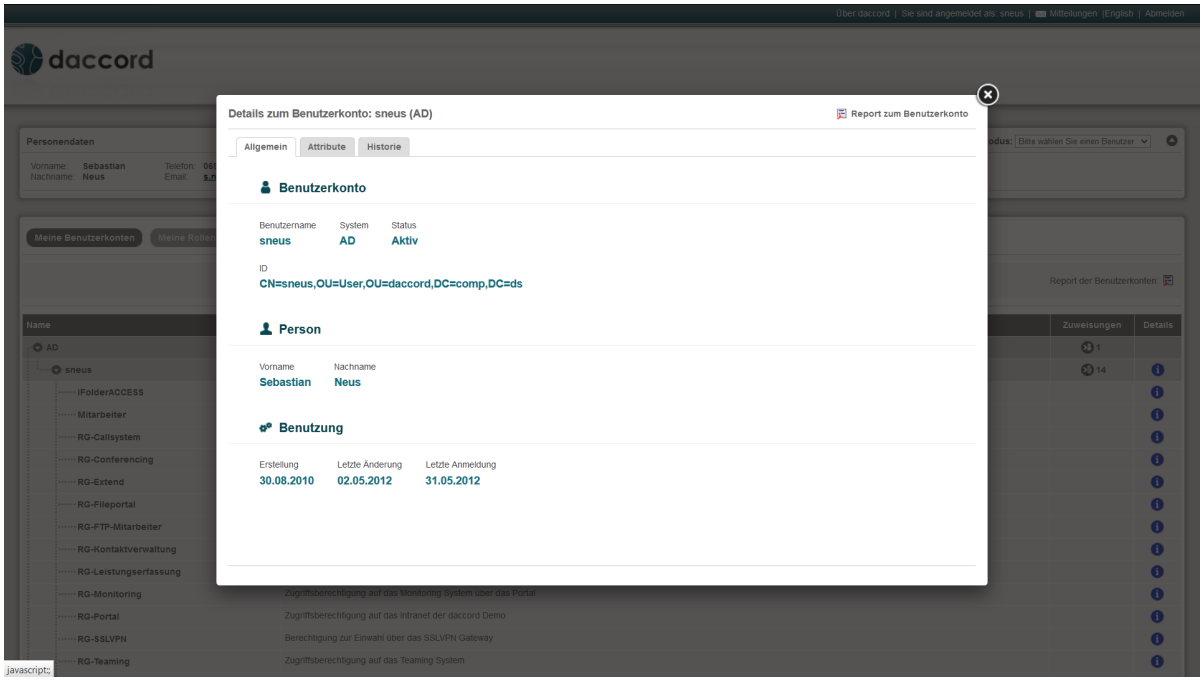


Abbildung 28: Allgemeine Informationen zu einem Benutzerkonto

In den folgenden Tabellen finden Sie eine kurze Erklärung der angezeigten Informationen.

Benutzerkonto

Parameter	Beschreibung
Benutzername	Benutzername des ausgewählen Benutzerkontos.
System	Name des Systems auf dem das Benutzerkonto eingerichtet ist.
Status	Gibt an ob das Benutzerkonto aktiv ist.
ID	Gibt die ID des Benutzerkontos auf dem Zielsystem an.

Tabelle 15: „Allgemein"-Tab: Informationen zum Benutzerkonto

Person

Parameter	Beschreibung
Vorname	Vorname der Person, der das Benutzerkonto bzw. die Berechtigung zugeordnet ist.
Nachname	Nachname der Person, der das Benutzerkonto bzw. die Berechtigung zugeordnet ist.

Tabelle 16: „Allgemein"-Tab: Informationen zur Person

Benutzung

Parameter	Beschreibung
Erstellung	Erstellungsdatum des Benutzerkontos
Letzte Änderung	Letzte Änderung des Benutzerkontos
Letzte Anmeldung	Letzte Anmeldung am Benutzerkonto.

Tabelle 17: „Allgemein"-Tab: Informationen zur Benutzung

Berechtigung

Parameter	Beschreibung
ID	Gibt die ID der Berechtigung an.
System	Name des Systems auf dem die Berechtigung eingerichtet ist.
Beschreibung	Optionale Beschreibung der Berechtigung.

Tabelle 18: „Allgemein"-Tab: Informationen zur Berechtigung

4.2 Zertifizierung

In dem „Zertifizierung"-Tab werden alle Informationen zur Zertifizierung angezeigt. Es wird z.B. angezeigt, ob und wie lange die Berechtigung oder Rollen-Zuweisung zertifiziert ist. Ist die Zertifizierung unbeschränkt, wird bei "Fällig am" kein Datum sondern der Text "keine Begrenzung" angezeigt.

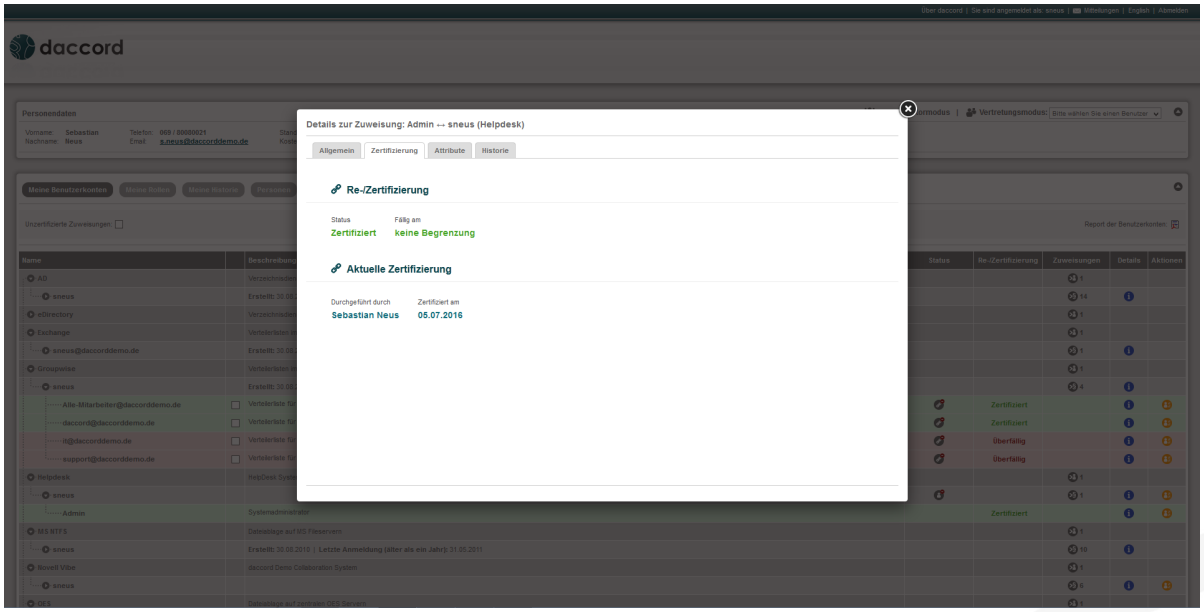


Abbildung 29: Detail-Ansicht der Zertifizierung

4.3 Attribute

In dem „Attribute"-Tab werden alle Attribute und dessen Werte ausgegeben, die daccord vom Zielsystem ausgelesen und gespeichert hat.

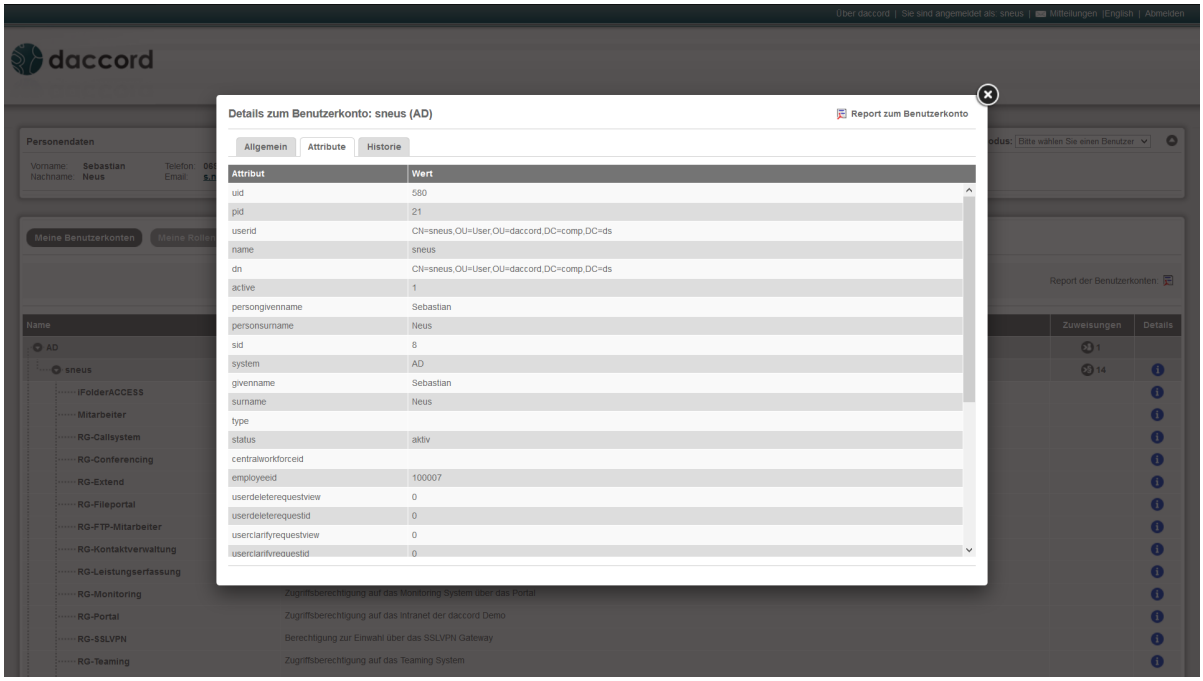


Abbildung 30: Übersicht der Attribute die aus dem Zielsystem von daccord ausgelesen wurden

4.4 Zuweisungen

In der Sichtweise „Benutzerkonten" können die Berechtigungszuweisungen eines Benutzerkontos ausgewertet werden. Die Anzahl der jeweiligen Zuweisungen wird in der Spalte „Zuweisungen" angezeigt. Neben der Anzahl der Zuweisungen befindet sich ein grünes Icon. Mit einem Klick auf dieses Icon, werden die Zuweisungen aufgelistet.

Hinweis: *Das Tab „Zuweisungen" wird nur in den beiden Sichtweisen „Benutzerkonten" und „Berechtigungen" unter der Kategorie „Systeme" angezeigt.*

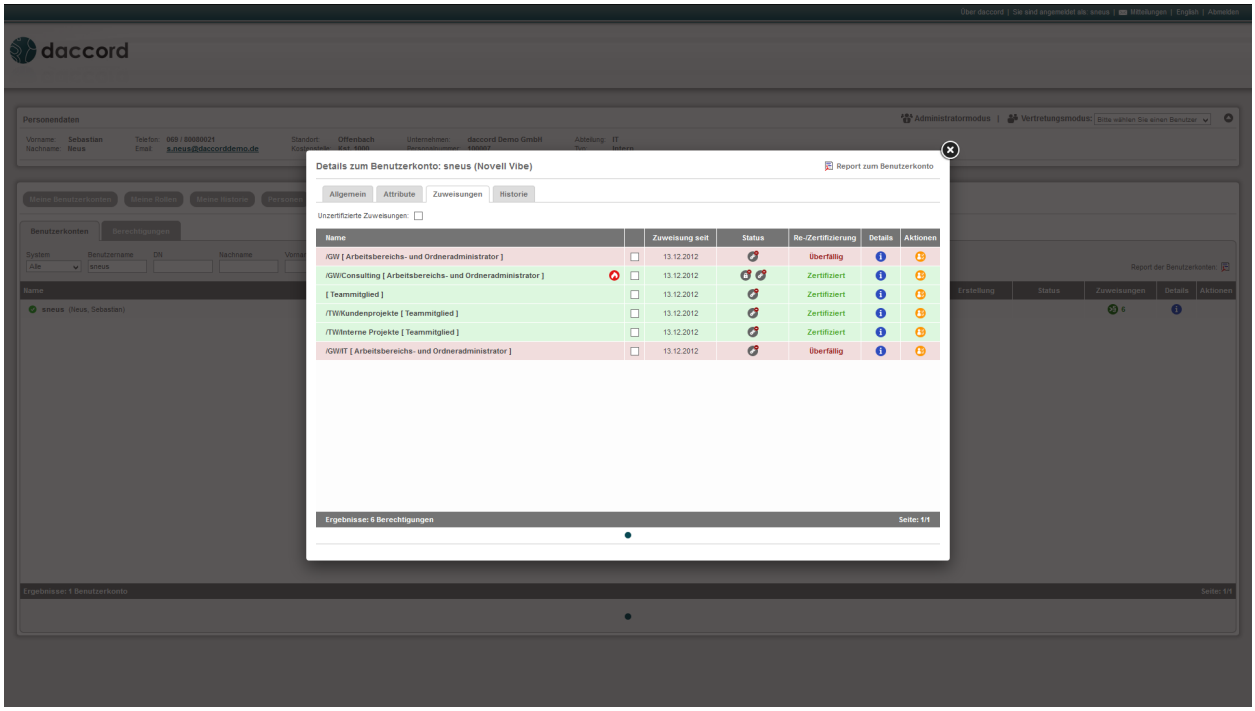


Abbildung 31: Auflistung der zugewiesenen Berechtigungen zu einem Benutzerkonto

Hinweis: *Um einen Report über alle Berechtigungen des ausgewählten Benutzerkontos zu ziehen, klicken Sie oben rechts oberhalb der Auflistung auf „Report zum Benutzerkonto". Darauf hin wird eine PDF generiert und zum Download angeboten.*

In der folgenden Tabelle werden die einzelnen Spalten der Ansicht „Zuweisungen" kurz erklärt.

Parameter	Beschreibung
Name	Zeigt den Namen der Zuweisung an.
Zuweisung seit	Gibt an, seit wann die Berechtigung dem Benutzerkonto zugewiesen ist,
Status	Wurde für diese Berechtigung eine Aktion angestoßen (z.B. Löschen) und befindet sich diese noch in der Bearbeitung, wird an dieser Stelle ein entsprechendes Icon angezeigt.
Details	Erlaubt das Öffnen der Details einer Berechtigung.
Aktionen	Sofern für ein Berechtigung eine Aktion möglich ist, kann diese über das orange „Aktion"-Icon angestoßen werden. Folgende Aktionen sind möglich: • Löschen - Die hinterlegte Aktion zum Löschen einer Berechtigung wird ausgeführt • Klären - Die hinterlegte Aktion zum Klären einer Berechtigung wird ausgeführt • Re-/Zertifizierung - Die hinterlegte Aktion zum Re-/Zertifizierung einer berechtigung wird ausgeführt

Tabelle 19: Übersicht der Zuweisungen

4.5 Historie

Im Historie-Tag werden alle Prozesse und Systemereignisse des aufgerufenen Benutzerkontos bzw. der Berechtigung angezeigt.

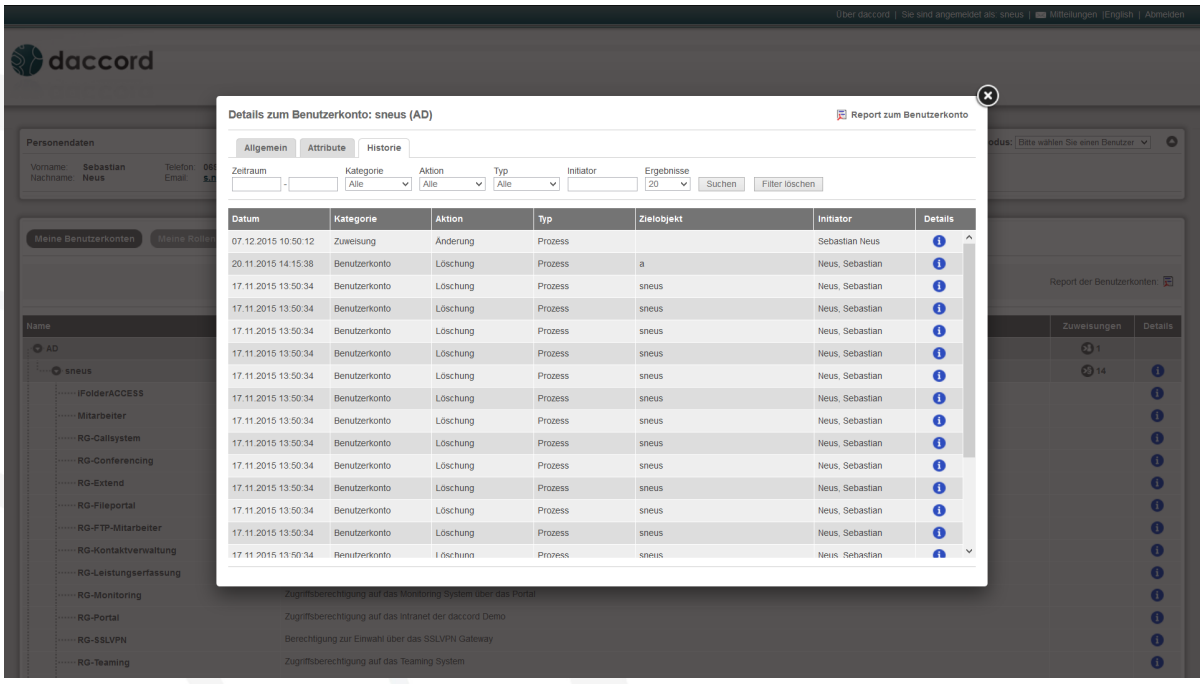


Abbildung 32: Übersicht aller zugeordneten Aktionen eines Benutzerkontos

Die Einträge in der Liste können nach verschiedenen Kriterien gefiltert werden. In der folgenden Tabelle, werden die Kriterien des Filters aufgeführt und kurz erläutert.

Parameter	Beschreibung
Startdatum	Filtert nach Aktionen, die ab dem angegebenen Datum erstellt wurden.
Enddatum	Filtert nach Aktionen, die bis zum angegebenen Datum erstellt wurden.
Kategorie	Wählen Sie zwischen den Kategorien... • Alle • Benutzerkonto • Zuweisung um die Suche einzugrenzen.
Aktion	Wählen Sie zwischen den Aktionen... • Erstellung • Löschung • Klärung • Änderung • Re-/Zertifizierung um die Suche einzugrenzen.
Typ	Wählen Sie zwischen den Typen... • Systemereignis • Prozess um die Suche einzugrenzen.
Initiator	Filtert Aktionen nach Initiator, die bis zum angegebenen Datum erstellt wurden.
Ergebnisse	Geben Sie an, wie viele Ergebnisse die Suche zurückliefern soll. Der Standartwert hierfür ist 20.

Tabelle 20: Filter für „Historie" zum Benutzerkonto

Die angezeigten Aktionen sind in die zwei Arten „Prozess" und „Systemereigniss" unterteilt. Zu jeder in der Liste aufgeführten Aktion, lassen sich die einzelnen Prozessschritte anzeigen. Klicken Sie dazu auf das blaue Info-Icon. Daraufhin werden die Prozessschritte eingeblendet. Um mehr über einen Prozessschritt zu erfahren, klicken Sie diesen an. Im unteren Bereich werden die Attribute und dessen Werte angezeigt, die zu diesem Prozessschritt von daccord gespeichert wurden.

In der Liste werden neben den Prozessen auch Systemereignisse angezeigt. Um sich die einzelnen Attribute anzeigen zu lassen, die zu diesem Systemereignis gespeichert wurden, klicken Sie auf das blaue Info-Icon. Zur besseren übersicht der einzelnen Attribute, sind diese in die Tabs „Allgemein", „Event Attribute", „User Attribute" und „Right Attribute" unterteilt.

Hinweis: *Lassen Sie sich für einen Prozess alle Prozessschritte in einem Report zusammen fassen. Klicken Sie dazu oben rechts auf das Icon „Report des Prozesses"*

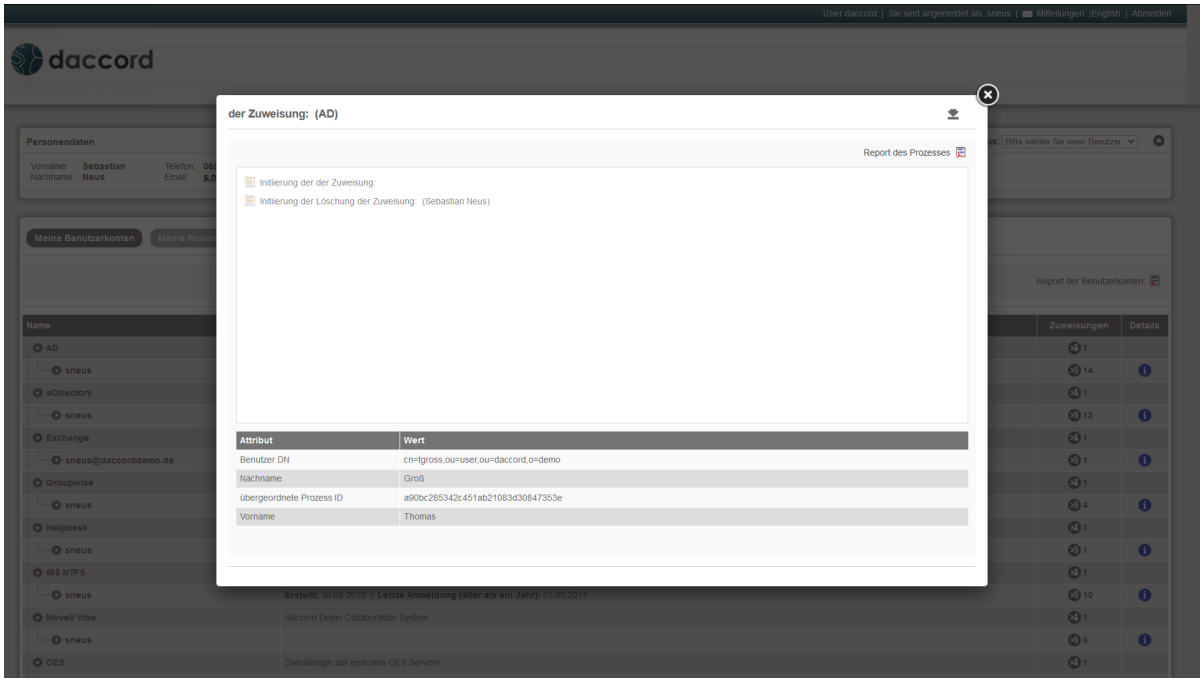


Abbildung 33: Diese Ansicht zeigt alle Prozessschritte zum ausgewählten Prozesses.

Hinweis: *Ein Klick auf den Pfeil (rechts oben in der Ecke) blendet die einzelnen Prozessschritte wieder aus, und Sie gelangen zur Übersicht.*

5 daccord User Frontend Aktionen

Für die Benutzerkonten und Berechtigungen können verschiedene Aktionen durchgeführt werden. Je nach Konfiguration wird beim Absenden eine Aktion ausgeführt (z.B. eine E-Mail verschickt oder eine Webservice-Schnittstelle eines anderen Systems angesprochen). Zu Benutzerkonten, Berechtigungen und Zuweisungen können über das daccord User Frontend Aktionen initiiert werden.

Je nachdem wie das daccord User Frontend konfiguriert ist, wird in den verschiedenen Übersichtslisten, die Spalte „Aktionen" angezeigt. Wenn für ein Benutzerkonto oder eine Berechtigung eine Aktion möglich ist, wird in dieser Spalte ein oranges Icon angezeigt.

Abbildung 34: Übersicht aller Aktionen eines ausgewählten Prozesses

Mit einem Klick auf dieses Icon öffnet sich ein Fenster. Die auszuführenden Aktionen werden in Form von Tabs dargestellt (Löschen, Klären, Re-/Zertifizieren) und können per Klick ausgewählt werden.

Hinweis: *Um eine Aktion für mehrere Berechtigungen eines Benutzerkontos gleichzeitig auszuführen, kann die Mehrfachauswahl genutzt werden. Dazu markieren Sie die gewünschten Checkboxen, bei denen eine Aktion ausgeführt werden soll und klicken dann auf das orange Icon des übergeordneten Benutzerkontos.*

5.1 Löschen

Um die Löschung eines Benutzerkontos oder einer Berechtigung zu beantragen, öffnen Sie das Tab „Löschen". Füllen Sie das Formluar aus, indem Sie einen Grund für die Löschung des jeweiligen Benutzerkontos oder Berechtigung angeben. Bestätigen Sie Ihre gewünschte Aktion mit einem Klick auf den Button „Senden". Je nach Konfiguration wird beim Absenden eine Aktion ausgeführt (z.B. eine E-Mail verschickt oder eine Webservice-Schnittstelle eines anderen Systems angesprochen).

Solange sich der Antrag in Bearbeitung befindet, wird dies in der Spalte Status in Form eines entsprechenden Icons graues Benutzersymbol) angezeigt.

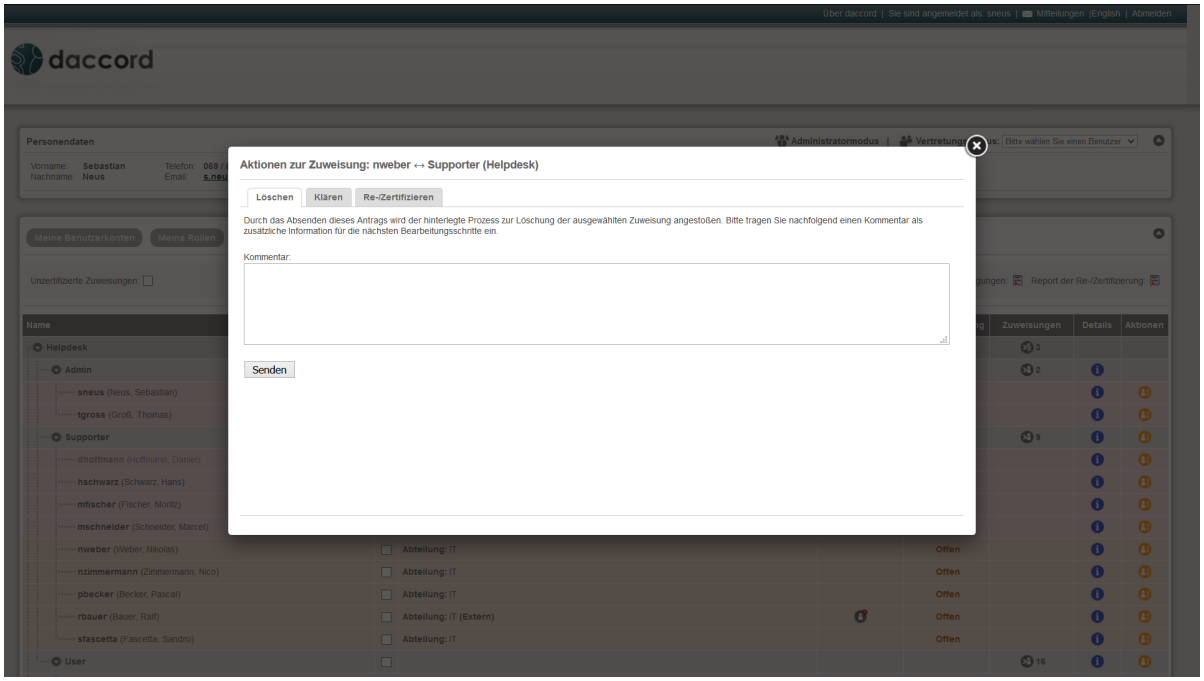


Abbildung 35: Formular zum Beantragen einer Löschung

Wurde eine Löschung bereits beantragt, kann diese nicht erneut beantragt werden. Es wird ein entsprechender Hinweis mit den Daten des bereits getätigten Antrages angezeigt.

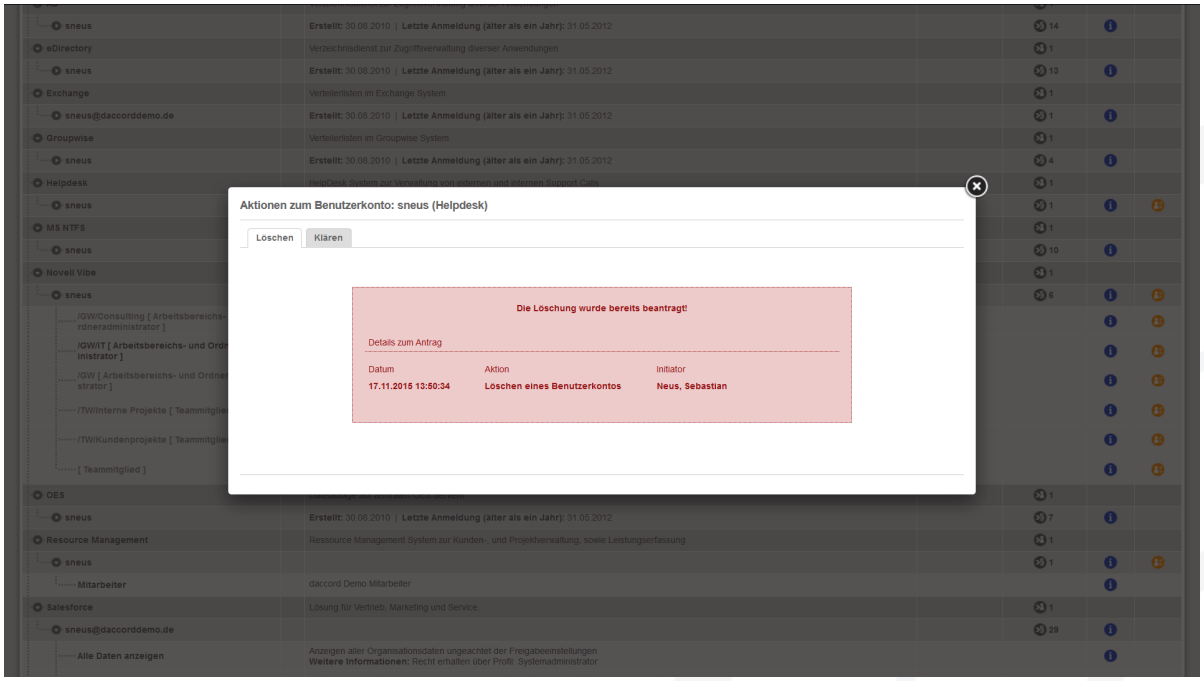


Abbildung 36: Meldung bei bereits beantragter Löschung

5.2 Klären

Um die Klärung eines Benutzerkontos oder einer Berechtigung zu beantragen, öffnen Sie das Tab „Klären". Das Formular zum Beantragen einer Klärung sieht ähnlich aus, wie das Formluar zum Beantragen einer Löschung. Tragen Sie den Grund für die gewünschte Klärung ein. Bestätigen Sie Ihre gewünschte Aktion mit einem Klick auf den Button „Senden". Je nach Konfiguration wird beim Absenden eine Aktion ausgeführt (z.B. eine E-Mail verschickt oder eine Webservice-Schnittstelle eines anderen Systems angesprochen).

Solange sich der Antrag in Bearbeitung befindet, wird dies in der Spalte „Status", in Form eines entsprechenden Icons (graues Rechtesymbol) angezeigt.

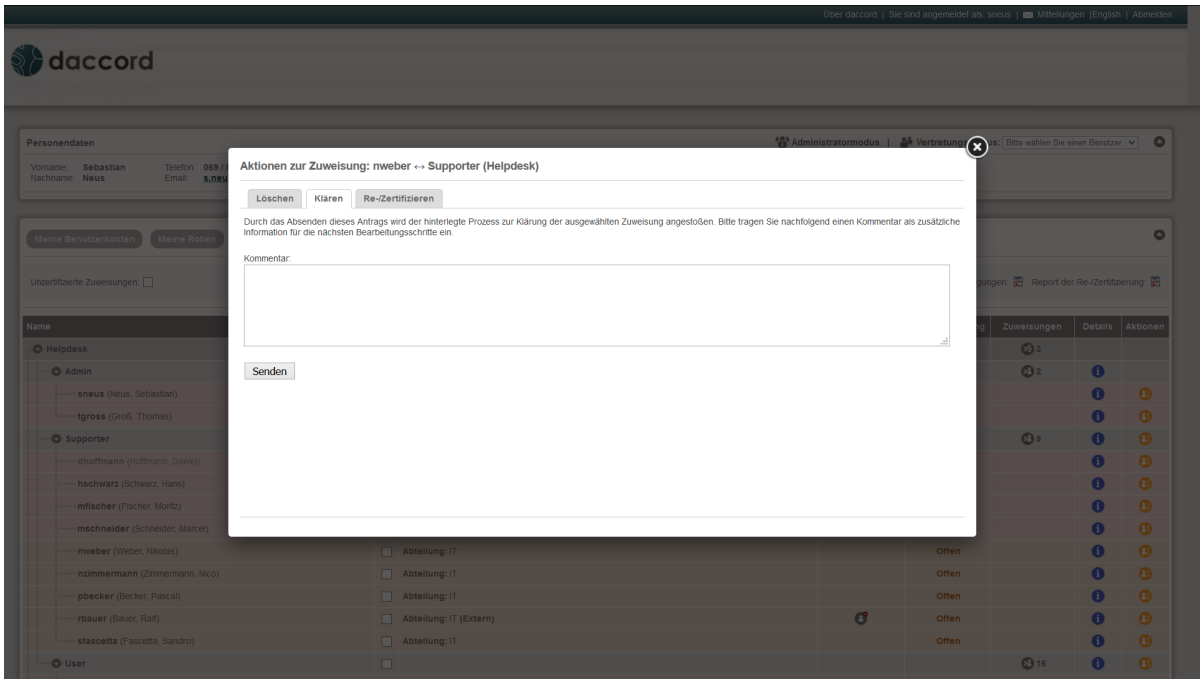


Abbildung 37: Formular zum Beantragen einer Klärung

5.3 Re-/Zertifizierung

Wenn die Re-/Zertifizierung aktiv ist, und der Anwender entsprechende Berechtigungen besitzt, können verschiedene Rechte und Zuweisungen re-/zertifiziert werden. Ist die Rollen-Zertifizierung eingeschaltet, lassen sich auch ganze Rollen und die über die jeweilige Rollen vergebenen Berechtigungen re-/zertifizieren.
Je nach Berechtigung, ist in den Tabs “Meine Benutzerkonten”, Meine Rollen”, “Systeme” und “Berechtigungen” eine Re-/Zertifizierung von Recht-Zuweisungen möglich. Eine genauere Beschreibung der Re-/Zertifizierung von Rechten und Berechtigungen finden Sie in den folgenden Kapitel (“5.3.1. Re-/Zertifizieren von Rechten”, “”5.3.2. Re-/Zertifizieren von Rollen”).

5.3.1 Re-/Zertifizierung von Rechten

Ist für eine Berechtigungszuweisung eine Zertifizierung notwendig, da es sich um eine neue Berechtigungszuweisung handelt oder das Re-/Zertifizierungsintervall überschritten wurde, kann über den Button “Aktionen” eine Re-/Zertifizierung durchgeführt werden.

Für die zu Re-/Zertifizierende Zuweisung kann ein individuelles Datum für die nächste Re-/Zertifizierung eintragen werden. Für die Auswahl des genannten Datums steht ausschließlich ein Zeitraum von heute bis zu dem vom System vorgegebenen Datum zur Verfügung. Neben dem Datum kann ein Kommentar zur Re-/Zertifizierung eingetragen werden.

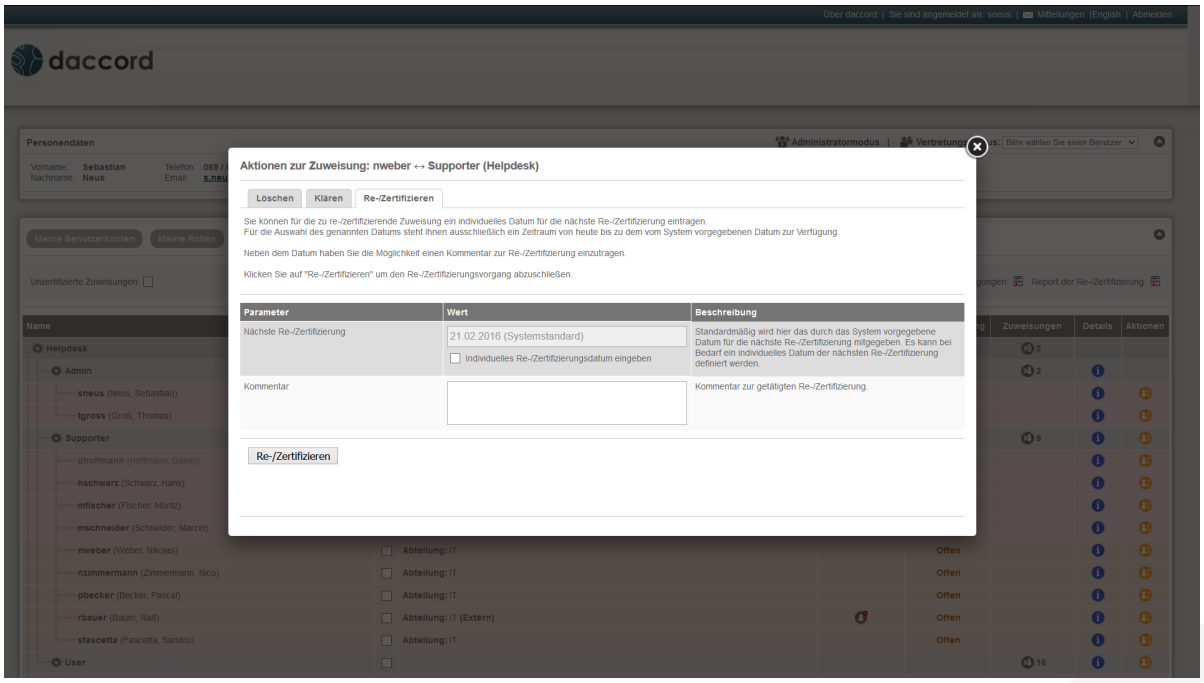


Abbildung 38: Formular zur Re-/Zertifizierung

5.3.2 Re-/Zertifizierung von Rollen

Ist die Rollen-Zertifizierung aktiviert, muss das Rollenmodell an sich zertifiziert werden. Es muss bestätigt werden, dass die Berechtigungen, die über eine Rolle vergeben werden, zu dieser Rolle gehören. Der sogenannte „Role Manager" ist dafür verantwortlich, dass die einzelnen Teile des Rollenmodells re-/zertifiziert werden.

Ist der aktuell angemeldete Benutzer ein „Role Manager" wird ein "Rollenmanager"-Tab eingeblendet, über das die Rollen und die jeweils zugeordneten Berechtigungen aufgelistet werden. Die Rollen-Rechte-Zuweisungen können vom Rollen-Manager re-/zertifiziert werden, sofern die Rollen-Zertifizierung aktiviert ist.

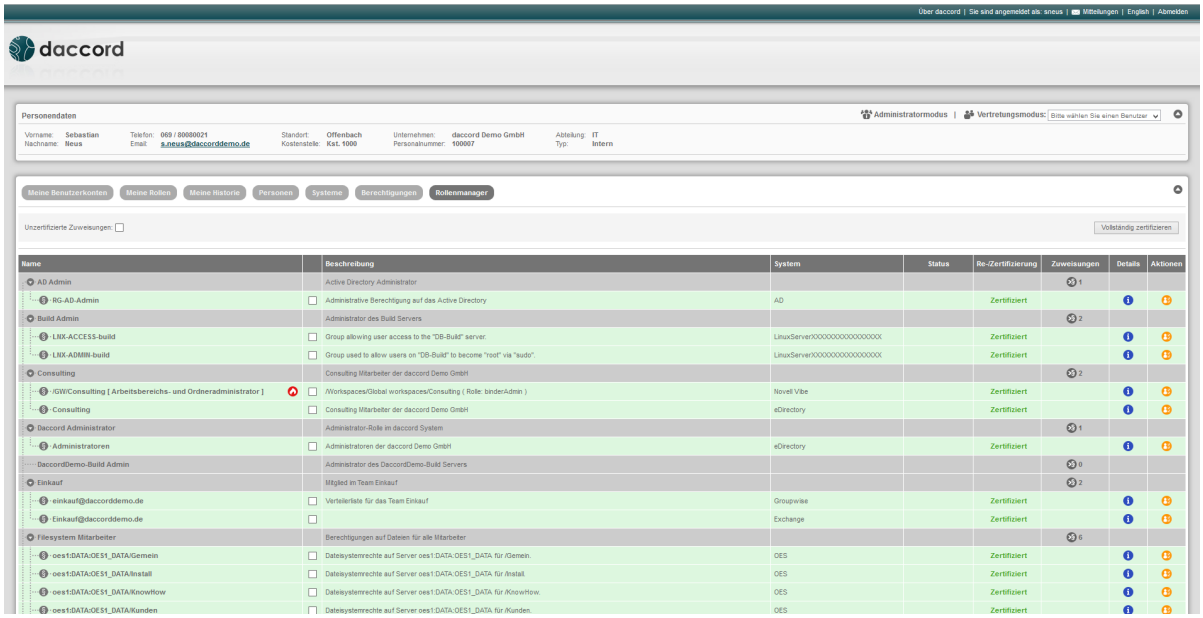


Abbildung 39: Übersicht "Rollenmanager"

Ist für eine Rolle eine Zertifizierung notwendig, da es sich um eine neue Rolle handelt oder das Re-/Zertifizierungsintervall überschritten wurde, kann über den Button "Aktionen" eine Re-/Zertifizierung durchgeführt werden.

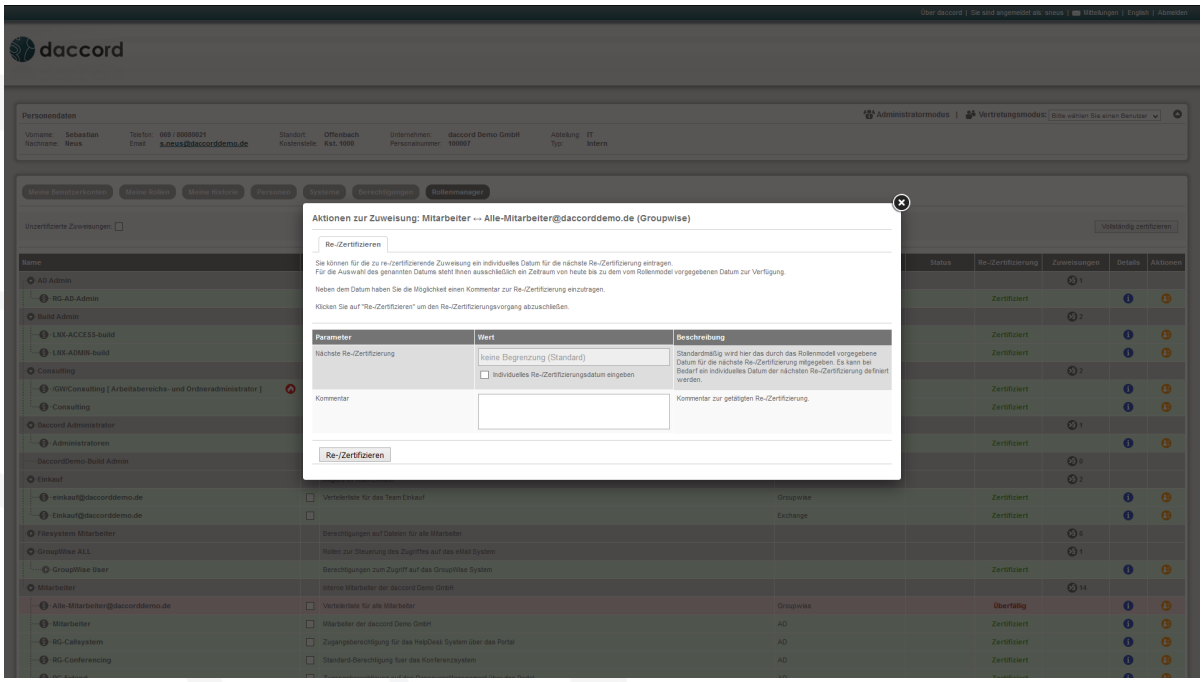


Abbildung 40: Formular zur Re-/Zertifizierung einer Rolle

Für die zu Re-/Zertifizierende Rollen-Zuweisung kann ein individuelles Datum für die nächste Re-/Zertifizierung eintragen werden. Für die Auswahl des genannten Datums steht ausschließlich ein Zeitraum von heute bis zu dem vom System vorgegebenen Datum zur Verfügung. Neben dem Datum kann ein Kommentar zur Re-/Zertifizierung eingetragen werden.

Die Berechtigungen, die Personen über Rollen erhalten haben, werden nur durchgängig zertifiziert, wenn die Rollen mit den zugewiesenen Berechtigungen vom Role-Manager zertifiziert wurden und der Person-Manager die Rollen-Personenzuweisung zertifiziert hat (siehe dazu Kapitel “5.3.3. Re-/Zertifizierung von Rollen-Zuweisungen”).

Zertifziert der Person-Manager die Rollen-Personenzuweisung zu einem Zeitpunkt, an dem der Role-Manager die Rollen-Rechtezuweisung noch nicht zertifiziert hat, wird nur die Rollen-Personenzuweisung zertifiziert. Erst wenn der Role-Manager die Rollen-Rechtezuweisungen zertifiziert, werden die Berechtigungen der Person automatisch zertifiziert.

5.3.3 Re-/Zertifizierung von Rollen-Zuweisungen

In den Details zur Person werden unter “Rollen” -> “Zugewiesene Rollen” die Rollen angezeigt, die der jeweiligen Person gerade zugeordnet sind.

Ist die Re-/Zertifizierung aktiviert, können die Rollen-Zuweisungen vom Person-Manager re-/zertifiziert werden. Mit einem Klick auf das “Aktion”-Icon öffnet sich eine Lightbox. Dort wählen Sie nun den “Re-/Zertifizierung”-Tab aus. Ist das Datum abgelaufen, muss diese Rollen-Zuweisung geprüft und gegebenen falls gelöscht oder ein Datum für die nächste Re-/Zertifizierung hinterlegt werden.

Es wird ebenfalls dargestellt, welche Berechtigungszuweisungen die jeweiligen Personen aufgrund der Rollenzuweisung in den Zielsystemen haben sollen. Ist der Rolle ein Recht zugewiesen, bei der eine Zuweisung fehlt, wird vor dem Recht ein rotes Icon mit einem “X” angezeigt. Weisen ein oder mehrere Rechte eine fehlende Zuweisung auf, wird bei der übergeordneten Rolle, ein oranges Warnzeichen angezeigt. Sind in der Übersicht z.B. alle Rollen zugeklappt, können Sie anhand des Warnzeichens erkennen, bei welchen Rollen es Probleme mit der Zuweisung von Rechten gibt.

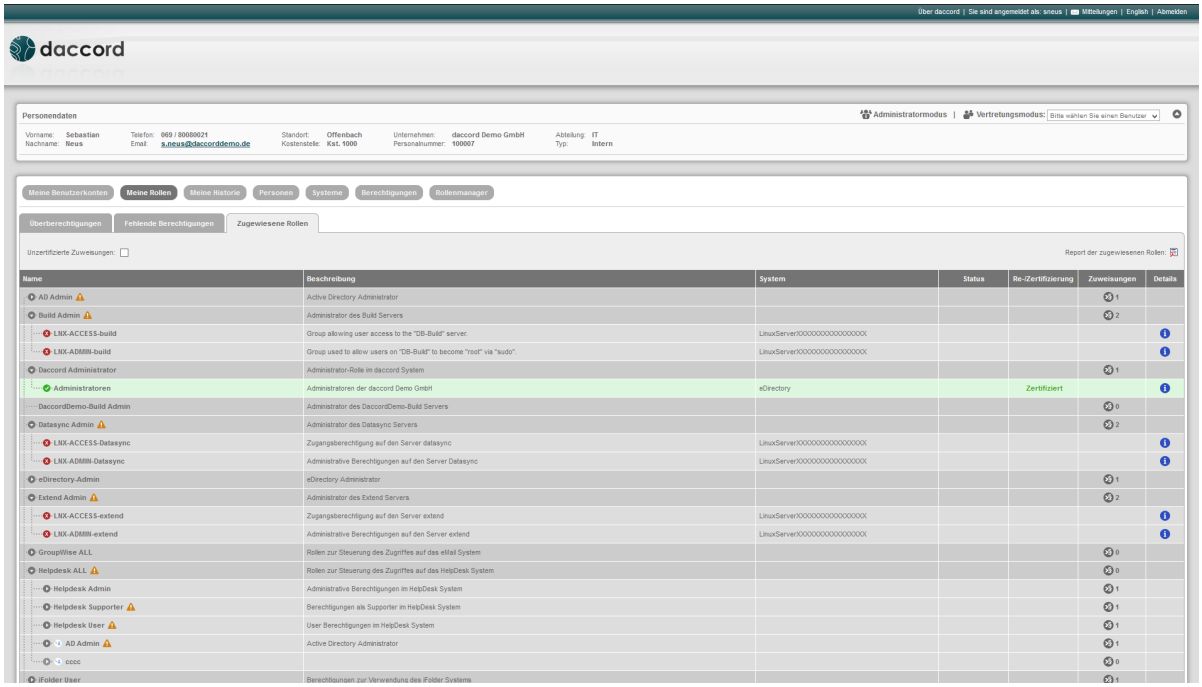


Abbildung 41: Übersicht “Zugewiesene Rollen”

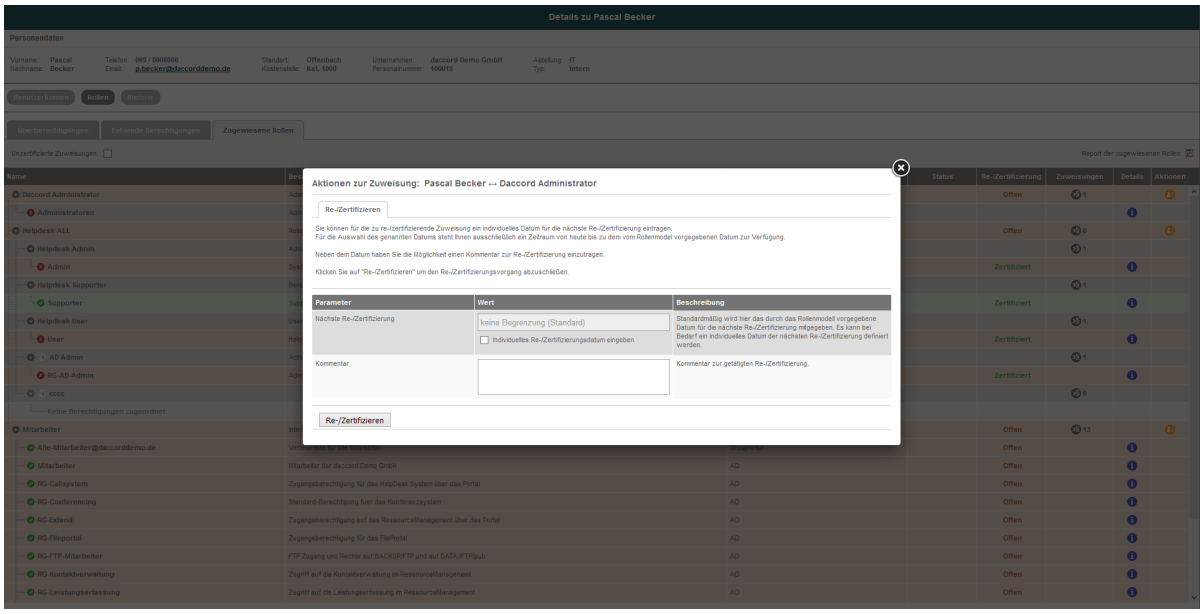


Abbildung 42: Formular zur Re-/Zertifizierung

Für die zu Re-/Zertifizierende Rollen-Zuweisung kann ein individuelles Datum für die nächste Re-/Zertifizierung eingetragen werden. Für die Auswahl des genannten Datums steht ausschließlich ein Zeitraum von heute bis zu dem vom System vorgegebenen Datum zur Verfügung. Neben dem Datum kann ein Kommentar zur Re-/Zertifizierung eingetragen werden.

Neben der Zertifizierung von Rollen-Personenzuweisungen, muss auch das Rollenmodell an sich zertifiziert werden. Mehr zur Zertifizierung des Rollenmodels finden Sie im vorherigen Kapitel “5.3.2 Re-/Zertifizierung von Rollen”.

5.3.4 Re-/Zertifizierung zurücksetzen

Ist eine Recht, Rolle oder Rollen-Zuweisung bereits zertifiziert, kann diese Zertifizierung auch wieder zurück genommen werden. Klicken Sie dazu auf das “Aktion”-Icon und öffnen das “Re-/Zertifizierung”-Tab. In der sich öffnenden Lightbox, wird im oberen Bereich eine Message mit einem Button angezeigt. Klicken Sie auf den “Re-/Zertifizierung zurücksetzen”-Button um die Zertifizierung zurück zu nehmen.

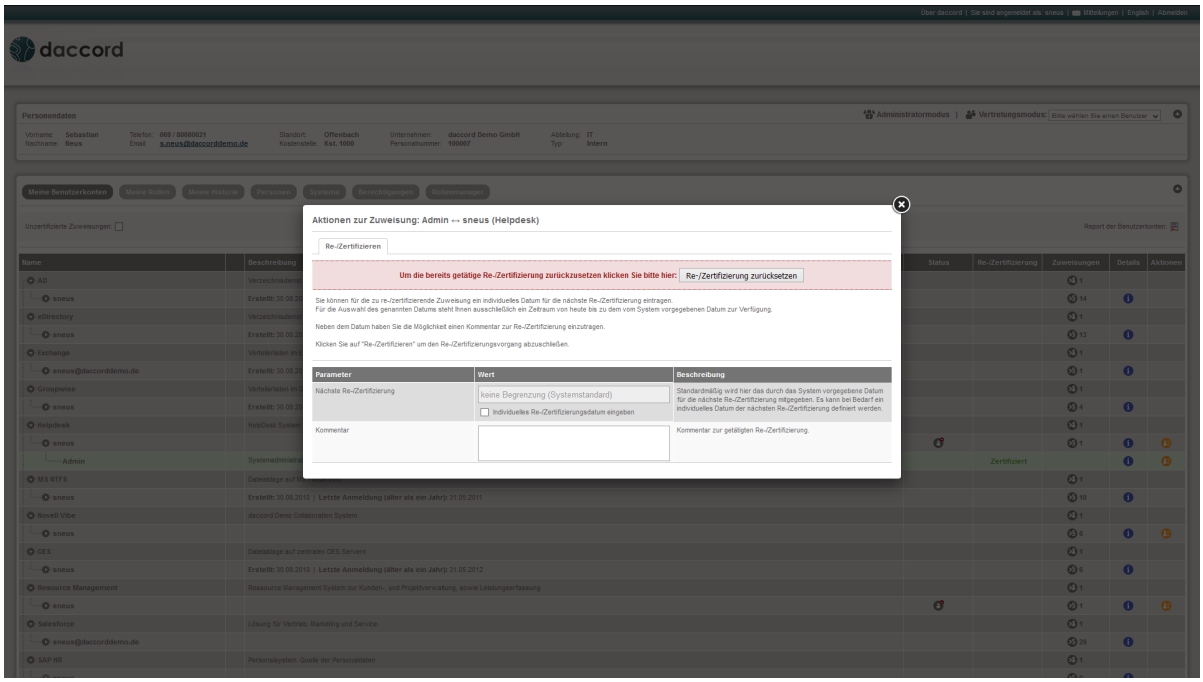


Abbildung 43: Re-/Zertifizierung zurücksetzen

6 Glossar

Wort	Beschreibung
„Person Manager"	Der „Person Manager" ist verantwortlich für einen bestimmten Personenkreis. Er kann dessen Konten und Berechtigungen einsehen und gegebenenfalls die Löschung eines Benutzerkontos oder einer Berechtigungszuweisung, einer Person die ihm zugewiesen ist, beantragen.
„Right Manager"	Ist verantwortlich für kritische Berechtigungen (z.B. spezielle Adminberechtigungen) die speziell überwacht werden müssen.
„Role Manager"	Der „Role Manager" ist für die Richtigkeit des Rollen-Modells zuständig und muss dieses re-/zertifizieren.
„System Manager"	Der „System Manager" ist für alle Benutzerkonten, Berechtigungen und Berechtigungszuweisungen eines Systems verantwortlich.
Rezertifizierung	Berechtigungszuweisung können im daccord System einer zyklischen Bestätigung der Korrektheit unterliegen. Diese Bestätigung wird als Re-/Zertifizierung bezeichnet.
Aktion	Über eine Aktion z.B. Löschen, Klären und Re-/Zertifizierung können verschiedene Aktivitäten im daccord System oder über RequestHandler in angeschlossenen, externen Systemen initiiert werden.
Prozess	Ein Prozess beschreibt im daccord System eine Abfolge von Informationen zu einer Aktion. Dabei können sowohl daccord interne Prozesse wie z.B. eine Re-/Zertifzierung, sowie externe Prozesse wie z.B. Löschung über eine E-Mail Benachrichtigung abgebildet werden.
Systemereignis	Dabei handelt es sich um ein Ereignis, welches von einem Collector ausgeführt wurde.
Collector	Ein Collector (to collect = dt. einsammeln) beinhaltet alle benötigten Informationen, um verwertbare Daten aus einem System zu holen.
Person	Eine Person (dt. Person) ist eine natürliche Person mit ihren Eigenschaften (Stammdaten). Eine Person kann beliebig viele Useraccounts (dt. Benutzerkonten) in den verschiedenen Systemen und Anwendungen besitzen und somit Zugriff auf diese haben.
Right	Ein Right (dt. Recht) ist eine Zugriffsberechtigung auf ein bestimmtes System oder eine bestimmte Anwendung. innerhalb einer IT-Landschaft im Unternehmen. Der Report kann entweder ausgehend von der jeweiligen Berechtigung erstellt werden, der dann aufzeigt, wer das jeweilige Recht besitzt. Oder ausgehend vom jeweiligen User, stellt der Report dar, welche Rechte dem User zugeordnet sind.

Wort	Beschreibung
Rolle	Mehrere zusammen gefasste Berechtigungen, um einzelne Berechtigungen nicht für jeden Nutzer einzeln festlegen zu müssen.
Rollen-Personen-Zuweisung	Gibt an, welche Rolle einer Person zugeordnet ist.
Rollen-Rechte-Zuweisung	Gibt an, welche Rechte einer Rolle zugewiesen ist.
Subrollen	Eine Rolle die einer anderen Rolle zugewiesen/untergeordnet ist.
System	Ein System ist eine Software bzw. Anwendung, in denen eine Person mit individuellen Berechtigungen aktiv ist.
Account	Bei einem Account (dt. Konto) handelt es sich um ein Benutzerkonto, das auf die Systeme zugreifen kann. Der Account ist damit ein Zugriffsrecht auf ein bestimmtes System. Es kann zwischen den aktiven und inaktiven Accounts unterschieden werden. Inaktive Benutzerkonten entstehen durch Mitarbeiterfluktuation, wenn zum Beispiel ein Mitarbeiter das Unternehmen verlässt oder die Abteilung wechselt.
daccord	daccord ist eine Software, die sämtliche Systeme des Unternehmens auf ihre Zugriffsrechte hin überprüfen kann. Dadurch werden die Rechtestrukturen des Unternehmens übersichtlich dargestellt und Rechteverletzungen aufgezeigt.
daccord Admin Frontend	Für administrative Tätigkeiten steht ein umfangreiches Admin Frontend zur Verfügung. Hierüber können alle Komponenten des Systems administriert werden. Zum Beispiel kann ein Collector mit anderen Parametern versehen oder ein ganz neuer Collector in das daccord-System hinzugefügt werden.
daccord User Frontend	Das webbasierte User Frontend von daccord dient der Darstellung von Informationen über Persons, User, Rights und Relations für den Anwender. Der Benutzer meldet sich über daccord an, wird authentisiert und kann direkt auf das User Frontend zugreifen, aus dem auch Reports verschickt werden können.
Report	Ein Report ist ein Bericht über die Zugriffsrechte
Zugriffsrecht	Mitarbeiter haben Zugriffsrechte, wenn ihnen erlaubt ist, ein System oder bestimmte Anwendungen für die tägliche Arbeit zu nutzen. Zugriffsrechte sollten nicht willkürlich vergeben werden, da dadurch Sicherheitslücken entstehen.

Tabellenverzeichnis

G+H Systems GmbH

Ludwigstraße 8
63067 Offenbach am Main

Tel.: +49 (0) 69 85 00 02-0
Fax: +49 (0) 69 85 00 02-51

Email: info@guh-systems.de
Web: www.guh-systems.de