

# System Configuration

## Benutzerverwaltung



## Administrationsanleitung

### für Systembetreiber

09.09.2020

*Originalanleitung*

### Produktlinie neo, Version 6.x

Die beschriebenen Funktionen können mit folgenden ASC-Produkten verwendet werden:

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

Im Partnerbereich unserer Webseite <http://www.asctechnologies.com> finden Sie immer die aktuellsten technischen Dokumente und Produktaktualisierungen.

Copyright © 2019 ASC Technologies AG. Alle Rechte vorbehalten.

Windows ist ein eingetragenes Markenzeichen der Microsoft Corporation. VMware® ist ein eingetragenes Markenzeichen von VMware, Inc. Alle anderen hier erwähnten Marken und Produktnamen sind das Eigentum ihrer jeweiligen Inhaber.



## Inhaltsverzeichnis

<b>1</b>	<b>Allgemeine Hinweise .....</b>	<b>6</b>
<b>2</b>	<b>Einleitung .....</b>	<b>7</b>
<b>3</b>	<b>LDAP .....</b>	<b>10</b>
3.1	Zertifikat installieren .....	10
3.2	Troubleshooting .....	11
<b>4</b>	<b>Mandanten-Modul .....</b>	<b>12</b>
4.1	Hauptansicht .....	12
4.1.1	Symbolleiste .....	12
4.2	Detailansicht .....	13
4.2.1	Detailansicht für Mandanten-Account des Systembetreibers .....	13
4.2.2	Detailansicht für normale Mandanten .....	15
4.2.3	Detailansicht für Wiederverkäufer .....	16
4.2.4	Registerkarte Details .....	17
4.2.4.1	Zeitzone hinzufügen .....	18
4.2.4.2	Gruppenfeld Systemerreichbarkeit .....	19
4.2.4.3	Gruppenfeld Adresse .....	20
4.2.4.4	Gruppenfeld Kontaktperson .....	21
4.2.5	Registerkarte Extensions .....	21
4.2.5.1	Extensions hinzufügen .....	22
4.2.5.2	Extensions entfernen .....	24
4.2.6	Registerkarte PBX-Agenten-IDs .....	25
4.2.6.1	PBX-Agenten-ID hinzufügen .....	26
4.2.6.2	PBX-Agenten-ID entfernen .....	28
4.2.7	Registerkarte Chat-IDs .....	28
4.2.7.1	Chat-ID hinzufügen .....	29
4.2.7.2	Chat-ID entfernen .....	31
4.2.8	Registerkarte Passwörter .....	31
4.2.8.1	Eintrag bearbeiten .....	36
4.2.9	Registerkarte Allgemeine Einstellungen .....	36
4.2.9.1	Gruppenfeld Inaktivität .....	37
4.2.9.2	Gruppenfeld SMTP-Account .....	38
4.2.9.3	Gruppenfeld SNMP-Agent .....	39
4.2.9.4	Gruppenfeld Login-Einstellungen .....	41
4.2.9.5	Gruppenfeld Sonstige Einstellungen .....	43
4.2.9.6	Gruppenfeld Nutzungsbedingungen .....	44
4.2.10	Registerkarte LDAP-Verbindungsdaten .....	44
4.2.10.1	LDAP-Verbindungsdaten bearbeiten .....	45
4.2.11	Registerkarte Web Service .....	46
4.2.11.1	Web Service für den Systembetreiber konfigurieren .....	46
4.2.11.2	Web Service für den Mandanten konfigurieren .....	48

4.2.11.3	Pfad der WSDL-Datei.....	52
4.2.11.4	Web Service für den Wiederverkäufer konfigurieren .....	52
4.2.12	Registerkarte PBX.....	54
4.2.12.1	PBX zuweisen .....	55
4.2.12.2	PBX-Zuweisung entfernen .....	56
4.2.13	Registerkarte Systemlizenzen.....	56
4.3	Neuen Mandanten manuell anlegen .....	58
4.4	Mandanten manuell bearbeiten.....	59
4.5	Mandanten löschen .....	60
4.6	OAuth-Login für System aktivieren .....	60
<b>5</b>	<b>Angestellten-Modul .....</b>	<b>62</b>
5.1	Hauptansicht .....	62
5.1.1	Symbolleiste .....	63
5.1.1.1	Zusammenfassung anzeigen .....	64
5.1.1.2	Gesperrte Angestellte anzeigen .....	64
5.1.1.3	Angestellte sichtbar oder nicht sichtbar machen.....	65
5.1.1.4	Suchen .....	65
5.2	Detailansicht.....	66
5.2.1	Registerkarte Details .....	67
5.2.1.1	Gruppenfeld Daten des Angestellten .....	67
5.2.1.2	Gruppenfeld Adresse .....	70
5.2.1.3	Gruppenfeld Datenschutz und Nutzungsbedingungen .....	70
5.2.2	Registerkarte Account.....	71
5.2.2.1	Authentifizierung via LDAP .....	72
5.2.2.2	Kombinationsbenutzer zuordnen .....	73
5.2.2.3	Kombinationsbenutzer-Zuordnung löschen .....	74
5.2.3	Registerkarte Einstellungen .....	74
5.2.3.1	Gruppenfeld Berechtigungen .....	75
5.2.3.2	Gruppenfeld Protokollierungseinstellungen .....	76
5.2.4	Registerkarte Rollen.....	76
5.2.4.1	Rollen zuordnen .....	77
5.2.4.2	Rollenzuordnung löschen.....	77
5.2.5	Registerkarte Individuelle Funktionsrechte .....	78
5.3	Neuen Angestellten anlegen .....	79
5.4	Angestellten bearbeiten .....	80
5.5	Angestellten löschen .....	80
<b>6</b>	<b>Rollen-Modul .....</b>	<b>82</b>
6.1	Hauptansicht .....	82
6.1.1	Symbolleiste .....	82
6.2	Detailansicht.....	83
6.2.1	Registerkarte Details .....	84
6.2.2	Registerkarte Angestellte .....	84

6.2.2.1	Benutzer zuordnen.....	85
6.2.2.2	Benutzerzuordnung löschen .....	85
6.2.3	Registerkarte Funktionsrechte .....	85
6.3	Neue Rolle anlegen.....	87
6.4	Rolle duplizieren.....	87
6.5	Rolle bearbeiten .....	88
6.6	Rolle löschen.....	89
<b>7</b>	<b>Vordefinierte Funktionspakete .....</b>	<b>90</b>
7.1	Superuser anlegen.....	90
7.2	Superadmin anlegen .....	90
	<b>Abbildungsverzeichnis.....</b>	<b>92</b>
	<b>Tabellenverzeichnis .....</b>	<b>95</b>
	<b>Glossar .....</b>	<b>96</b>

**Allgemeine Hinweise**

ASC steht im Kontext dieses Dokuments für die ASC Technologies AG, deren Tochtergesellschaften, Niederlassungen und Vertriebsbüros. Deren aktuelle Übersicht kann auf der Webseite unter <https://www.asctechnologies.com> eingesehen werden.

ASC übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der in den Anleitungen bereitgestellten Informationen.

ASC kontrolliert regelmäßig den Inhalt der veröffentlichten Anleitungen auf Übereinstimmung mit der beschriebenen Hard- und Software. Dennoch können Abweichungen nicht ausgeschlossen werden. Notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Einige Aspekte der ASC-Technologie werden in allgemeiner Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von ASC zu schützen.

Die Softwareprogramme und Anleitungen von ASC sind urheberrechtlich geschützt. Alle Rechte an den Anleitungen sind vorbehalten, auch die der Reproduktion und/oder Vervielfältigung in jeglicher Form, sei es fotomechanisch, drucktechnisch oder auf digitalen Datenträgern. Dies gilt auch für Übersetzungen. Nachdruck der Anleitungen, vollständig oder auszugsweise, ist nur mit schriftlicher Genehmigung von ASC gestattet.

Maßgebend ist, soweit nicht anders angegeben, der technische Stand zum Zeitpunkt der Auslieferung von Software, Geräten und Anleitungen durch ASC. Technische Änderungen ohne gesonderte Ankündigung bleiben vorbehalten. Bisherige Anleitungen verlieren ihre Gültigkeit.

Es gelten die Allgemeinen Verkaufs- und Lieferbedingungen von ASC in ihrer jeweils gültigen Fassung.

Das neo-System ist als potientiell Multi-Mandanten-System konzipiert. D. h. es besteht die Möglichkeit, mehrere unterschiedliche Mandanten innerhalb eines Systems zu betreiben. Diese Mandanten werden vom Systembetreiber oder Wiederverkäufer angelegt und verwaltet. Die Administratoren der einzelnen Mandanten haben die Möglichkeit ihrerseits Benutzer anzulegen, Rollen zu definieren und Funktionsrechte zu verwalten (siehe Administrationsanleitung *System Configuration - Benutzerverwaltung für Mandanten*).

Jedes neo-System wird initial als 1-Mandanten-System mit einem vordefinierten Mandanten, dem 1st-Tenant, installiert. Auch der Systembetreiber wird automatisch als Mandant angelegt. Er ist aber nicht als Mandant im eigentlichen Sinne zu betrachten.

Für den jeweiligen Administrator des Systembetreibers und des vordefinierten Mandanten wird bei der Installation des Systems standardmäßig ein Account mit folgenden Login-Daten angelegt:

Login-Daten für den Administrator des Systembetreibers:

Benutzername:	<i>system-admin</i>
<u>neo</u> -Version < 6.3	
Standard-Passwort:	1
	Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version $\geq 6.3$ das Standard-Passwort 1 noch nie geändert wurde, muss beim nächsten Login das Passwort geändert oder durch erneute Eingabe bestätigt werden. Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version $\geq 6.3$ das Standard-Passwort schon einmal geändert wurde, wird das geänderte Passwort beibehalten.
<u>neo</u> -Version $\geq 6.3$	
Standard-Passwort:	A\$c123

Tab. 1: Login-Daten - Systembetreiber

Login-Daten für den Administrator des 1. Mandanten:

Benutzername:	<i>1st-tenant-admin</i>
<u>neo</u> -Version < 6.3	
Standard-Passwort:	1
	Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version $\geq 6.3$ das Standard-Passwort 1 noch nie geändert wurde, muss beim nächsten Login das Passwort geändert oder durch erneute Eingabe bestätigt werden. Wenn vor einer Softwareaktualisierung auf eine <u>neo</u> -Version $\geq 6.3$ das Standard-Passwort schon einmal geändert wurde, wird das geänderte Passwort beibehalten.
<u>neo</u> -Version $\geq 6.3$	
Standard-Passwort:	A\$c123

Tab. 2: Login-Daten - 1. Mandant

Je nach Lizenzierung wird das neo-System als 1-Mandanten-System oder als Multi-Mandanten-System betrieben. In einem 1-Mandanten-System gibt es nur den vordefinierten Mandanten, es können keine weiteren Mandanten angelegt werden. In einem Multi-Mandanten-System kann der Systembetreiber so viele zusätzliche Mandanten anlegen wie Mandanten-Lizenzen im System vorhanden sind.

Für den jeweiligen Administrator des Systembetreibers und des vordefinierten Mandanten wird bei der Installation des Systems standardmäßig ein Account mit folgenden Login-Daten angelegt:

### **Systembetreiber**

Der Systembetreiber ist für die allgemeine Systemkonfiguration zuständig.

Der Systembetreiber kann:

- ihm untergeordnete Mandanten oder Wiederverkäufer erstellen, löschen und verwalten.
- eigene Angestellte als Benutzer des Systems erstellen, löschen und verwalten.

Der Systembetreiber hat keinen Zugriff auf die Benutzerdaten der einzelnen Mandanten. Mandantenspezifische Daten kann nur der jeweilige Mandant selbst sehen und bearbeiten.

### **Wiederverkäufer**

Der Wiederverkäufer besitzt eingeschränkte Rechte eines Systembetreibers und Mandanten.

Der Wiederverkäufer kann:

- ihm untergeordnete Mandanten und Wiederverkäufer erstellen, löschen und verwalten.
- eigene Angestellte als Benutzer des Systems erstellen, löschen und verwalten.

Der Wiederverkäufer hat keinen Zugriff auf die Benutzerdaten der einzelnen Mandanten. Mandantenspezifische Daten kann nur der jeweilige Mandant selbst sehen und bearbeiten.

### **Mandant**

Der Mandant ist der Endkunde.

Der Mandant kann:

- eigene Angestellte als Benutzer des Systems erstellen, löschen und verwalten.

Diese Anleitung beschreibt, wie Sie als Systembetreiber folgende Konfigurationen durchführen können:

- Mandanten und Wiederverkäufer anlegen und verwalten
- Eigene Benutzer anlegen und verwalten
- Funktionsrechte für eigene Benutzer verwalten
- LDAP-Authentifizierung für eigene Benutzer einrichten

Die Durchführung der verschiedenen Funktionen zur Benutzerverwaltung erfolgt in den folgenden Modulen der Applikation System Configuration:

- Mandanten-Modul

Im Mandanten-Modul können Sie Mandanten und Wiederverkäufer anlegen und deren Daten verwalten.

Siehe [Kapitel "Mandanten-Modul", S. 12.](#)

- Angestellten-Modul

Im Angestellten-Modul können Sie Benutzer anlegen, deren Daten verwalten und Funktionsrechte vergeben.

Siehe [Kapitel "Angestellten-Modul", S. 62.](#)

- Rollen-Modul

Im Rollen-Modul können Sie verschiedene Rollen definieren, über die Sie Benutzern Funktionsrechte per Rollensystem zuordnen können.

Siehe [Kapitel "Rollen-Modul", S. 82.](#)





Sie können entweder einem Benutzer Rollen zuordnen (im Angestellten-Modul) oder einer Rolle Benutzer (im Rollen-Modul). Beide Vorgehensweisen führen zu dem Ergebnis, dass der Benutzer die Funktionsrechte der Rolle erhält.



Im Angestellten-Modul können Sie den Umfang der Funktionsrechte, die einem Benutzer über eine Rolle zugewiesen wurden, mit individuellen Funktionsrechten ergänzen.



Wenn Sie Funktionsrechte eines Benutzers oder ihm zugeordnete Rollen ändern, während dieser angemeldet ist, wirkt sich die Änderung erst aus, wenn der Benutzer sich abmeldet und erneut anmeldet.

Ein Benutzer erhält keine Benachrichtigung, wenn seine Funktionsrechte oder Rollen geändert wurden.



Grundlegende Informationen zur Bedienung der Applikation System Configuration finden Sie in der Bedienungsanleitung für Administratoren *Allgemeine Informationen System Configuration*.

Die Produktlinie *neo* unterstützt die Authentifizierung von Benutzern via **LDAP** (Lightweight Directory Access Protocol).

Um das Feature **LDAP** verwenden zu können, muss mindestens 1 konfigurierter **LDAP**-Server (z. B. ein Active Directory) zur Verfügung stehen, in dem die Benutzer angelegt sind, die das *neo*-Aufzeichnungssystem nutzen sollen. Benutzer müssen darin als *User* angelegt sein. Sie dürfen in jeder Kombination von Verzeichnissen innerhalb des **LDAP**-Servers vorhanden sein.

Wenn Sie die Authentifizierung via **LDAP** verwenden möchten, müssen Sie zunächst im Mandanten-Modul alle Verbindungen zu möglichen **LDAP**-Servern konfigurieren und die grundsätzliche **LDAP**-Authentifizierung aktivieren. Bei der Konfiguration der einzelnen Benutzer können Sie dann entscheiden, ob die Anmeldung des Benutzers über **LDAP** erfolgen soll.

- **LDAP**-Verbindungsdaten konfigurieren.  
Siehe Kapitel "Registerkarte **LDAP**-Verbindungsdaten", S. 44.
- **LDAP**-Authentifizierung grundsätzlich aktivieren.  
Siehe Kapitel "Gruppenfeld Login-Einstellungen", S. 41.
- **LDAP**-Authentifizierung für einzelne Benutzer aktivieren.  
Siehe Kapitel "Authentifizierung via **LDAP**", S. 72.



Für eine erfolgreiche Anmeldung am **LDAP**-Server muss das Authentifizierungsverfahren *Simple Authentication* auf dem **LDAP**-Server konfiguriert sein.



Wenn für einen Benutzer die Authentifizierung via **LDAP** aktiv ist, diese Authentifizierung aber nicht erfolgreich ist (z. B. weil der **LDAP**-Server nicht erreichbar oder die Kombination aus Benutzernamen und Passwort nicht bekannt ist), erfolgt eine lokale Authentifizierung gegen die Informationen, die in der Datenbank des Aufzeichnungssystems gespeichert sind. Deswegen ist auch bei aktivierter **LDAP**-Authentifizierung für jeden Benutzer die Angabe eines lokalen Passworts im Angestellten-Modul notwendig.



Für die Verbindung zum **LDAP**-Server kann das Verschlüsselungsprotokoll Secure Sockets Layer (**SSL**) verwendet werden.

### 3.1

#### Zertifikat installieren

Um eine verschlüsselte Verbindung nutzen zu können, müssen Sie das entsprechende Zertifikat auf dem Aufzeichnungsserver installieren. Verwenden Sie dazu das *Certificate Import Tool* von ASC.

1. Öffnen Sie den Windows Explorer.
2. Wechseln Sie in den Ordner *C:\Program Files (x86)\ASC\ASC Product Suite\scripts\*.
3. Führen Sie die Datei *certimporter.exe* als Administrator aus.
4. Wählen Sie in der Navigationsleiste den Menüpunkt *HTTPS Trust* aus.
5. Wählen Sie die Registerkarte *Import Trusted Certificate*.
6. Klicken Sie auf die Schaltfläche Symbol  neben dem Feld *Certificate X.509*.
7. Wählen Sie aus dem Explorer-Dialog das passende Zertifikat aus und klicken Sie auf die Schaltfläche *Open*.
8. Klicken Sie auf die Schaltfläche *Import*, um das Zertifikat zu installieren.
9. Eine Erfolgsmeldung erscheint, wenn das Zertifikat erfolgreich importiert ist.
10. Starten Sie den *Glassfish-Server (Enterprise Core)* neu, damit das Zertifikat übernommen wird.

## 3.2

## Troubleshooting

**LDAP-SSL-Verbindung funktioniert nicht**

Das Zertifikat, das Sie auf dem Aufzeichnungsserver installieren, muss das gleiche Zertifikat sein, das auch auf dem LDAP-Server vorhanden ist. Unterscheiden sich die Zertifikate, kann die Verbindung nicht erfolgreich aufgebaut werden. Das führt dazu, dass LDAP SSL nicht verwendet werden kann.

## 4 Mandanten-Modul

Im Mandanten-Modul können Sie Mandanten oder Wiederverkäufer anlegen und deren Daten verwalten. Hier werden Kontaktdaten und zugewiesene Extensions verwaltet.

Das *neo*-System ist als potientes Multi-Mandanten-System konzipiert. Jedes System wird initial als 1-Mandanten-System mit 1 vordefinierten Mandanten, dem *1st-Tenant*, installiert. Auch der Systembetreiber wird automatisch als Mandant angelegt (Mandantenname = *System*). Er ist aber nicht als Mandant im eigentlichen Sinne zu betrachten. Abhängig von den vorhandenen Lizenzen können Sie hier im Mandanten-Modul weitere Mandanten oder Wiederverkäufer anlegen. Die Anlage neuer Mandanten oder Wiederverkäufer können Sie über den Web Service automatisiert durchführen oder manuell vornehmen.

Öffnen Sie das Mandanten-Modul, indem Sie in der Navigationsleiste der Applikation System Configuration auf den Menüpunkt *Mandanten* klicken.

### 4.1 Hauptansicht

In der Hauptansicht werden alle gespeicherten Mandanten angezeigt.

+ × Mandanten Allgemein ▾					
Name ▾	Kunden-ID ↕	Typ	Land ↕	Erstelldatum ↕	Aktualisiert ↕
▾ System		Systembetreiber		28.02.2011 15:20:52	06.11.2018 11:56:38
1st-tenant		Mandant		01.01.2012 13:00:00	06.11.2018 12:39:52
2nd-Tenant		Mandant		01.01.2012 13:00:00	06.11.2018 12:39:52
3rd-Tenant		Mandant		01.01.2012 13:00:00	06.11.2018 12:39:52

Abb. 1: Mandanten-Modul - Hauptansicht

<i>Name</i>	Name, mit dem der Mandant im System angezeigt wird.
<i>Kunden-ID</i>	Kunden-ID des Mandanten.
<i>Typ</i>	Zeigt den Mandantentyp an. <ul style="list-style-type: none"> <li>• Mandant</li> <li>• Wiederverkäufer</li> </ul>
<i>Land</i>	Land der Adresse des Mandanten.
<i>Erstelldatum</i>	Datum, an dem der Mandant angelegt wurde.
<i>Aktualisiert</i>	Datum, an dem die Daten des Mandanten zuletzt aktualisiert wurden.

#### 4.1.1 Symbolleiste

Die Symbolleiste bietet folgende Funktionen.

+ × Mandanten Allgemein ▾
---------------------------

Abb. 2: Mandanten-Modul - Symbolleiste

+	<i>Hinzufügen</i>	Legt einen neuen Mandanten oder Wiederverkäufer an (siehe <a href="#">Kapitel "Neuen Mandanten manuell anlegen"</a> , S. 58).
×	<i>Löschen</i>	Löscht den ausgewählten Mandanten (siehe <a href="#">Kapitel "Mandanten löschen"</a> , S. 60).
Mandanten		Dieses Menü steht zurzeit nicht zur Verfügung.

<i>Allgemein</i>	<i>Allgemeine Hilfe</i>	Über den Menüpunkt <i>Allgemeine Hilfe</i> wird eine Beschreibung der Applikation, in der Sie sich gerade befinden, geöffnet.
	<i>Modul-Hilfe</i>	Über den Menüpunkt <i>Modul-Hilfe</i> wird eine Beschreibung des Moduls, in dem Sie sich gerade befinden, geöffnet.



Detaillierte Beschreibungen zu Standardfunktionen wie z. B. *Drucken*, *Tabelle anpassen* oder *Hilfe* finden Sie in der Bedienungsanleitung für Administratoren *Allgemeine Informationen zur System Configuration*.

## 4.2

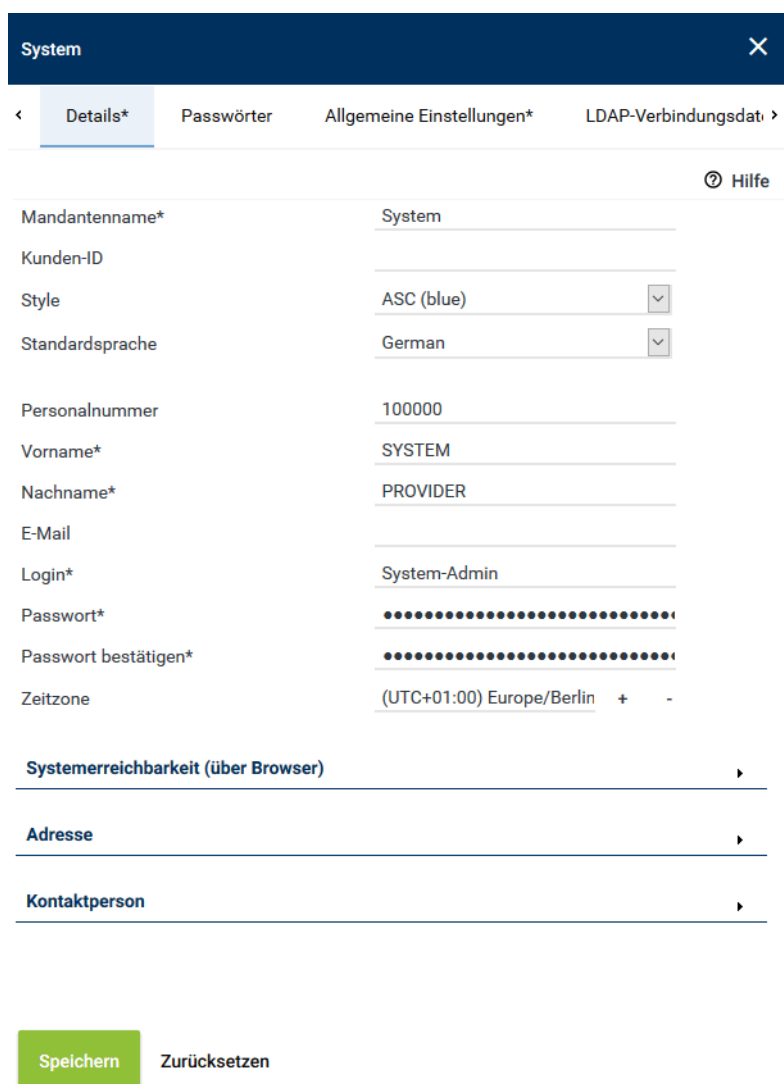
### Detailansicht

Die Detailansicht enthält weitere Informationen und Funktionen zum ausgewählten Mandanten oder Wiederverkäufer. Der Inhalt der Detailansicht hängt davon ab, ob in der Hauptansicht der Mandanten-Account des Systembetreibers ausgewählt wurde oder der Account eines beliebigen anderen Mandanten.

Die Registerkarte *Details* ist für alle Mandanten oder Wiederverkäufer gleich, unabhängig davon, ob es sich um den Mandanten-Account des Systembetreibers, einen normalen Mandanten oder einen Wiederverkäufer handelt.

### 4.2.1

#### Detailansicht für Mandanten-Account des Systembetreibers



**System** [X]

< **Details\*** Passwörter Allgemeine Einstellungen\* LDAP-Verbindungsdati >

② Hilfe

Mandantename\* System

Kunden-ID

Style ASC (blue) [v]

Standardsprache German [v]

Personalnummer 100000

Vorname\* SYSTEM

Nachname\* PROVIDER

E-Mail

Login\* System-Admin

Passwort\* .....

Passwort bestätigen\* .....

Zeitzone (UTC+01:00) Europe/Berlin + -

**Systemerreichbarkeit (über Browser)** ▶

**Adresse** ▶

**Kontaktperson** ▶

**Speichern** Zurücksetzen

Abb. 3: Mandanten-Modul - Detailansicht für den Mandanten "System"

Die Detailansicht besteht aus folgenden Registerkarten:

- *Details*

Hier können Sie Ihre Kontaktdaten für den Systembetreiber anzeigen und bearbeiten.

Siehe [Kapitel "Registerkarte Details", S. 17.](#)

- *Passwörter*

Hier können Sie die Passwortregeln definieren, die von den Benutzern berücksichtigt werden müssen, wenn sie ein Passwort anlegen.

Siehe [Kapitel "Registerkarte Passwörter", S. 31.](#)

- *Allgemeine Einstellungen*

Hier können Sie allgemeine Einstellungen (Inaktivität, Benachrichtigungseinstellungen, SSO-Login) vornehmen.

Siehe [Kapitel "Registerkarte Allgemeine Einstellungen", S. 36.](#)

- *LDAP-Verbindungsdaten*

Hier können Sie LDAP-Verbindungen konfigurieren.

Siehe [Kapitel "Registerkarte LDAP-Verbindungsdaten", S. 44.](#)

- *Web Service*

Hier können Sie die Verwendung des Web Service konfigurieren.

Siehe [Kapitel "Registerkarte Web Service", S. 46.](#)

### 4.2.2 Detailansicht für normale Mandanten

1st-tenant

Details\*

Extensions

PBX-Agenten-IDs

Chat-IDs

Web Service

Hilfe

Mandantenname*	1st-tenant
Kunden-ID	
Style	ASC (blue) <span>▼</span>
Standardsprache	Deutsch <span>▼</span>
Personalnummer	200000
Vorname*	1st-Tenant
Nachname*	Admin
E-Mail	
Login*	1st-Tenant-Admin
Passwort*	.....
Passwort bestätigen*	.....
Account sperren	<input type="checkbox"/>
Zeitzone	(UTC+01:00) Europe/Berlin + -

Systemerreichbarkeit (über Browser)

Adresse

Kontaktperson

Speichern

Zurücksetzen

Abb. 4: Mandanten-Modul - Detailansicht für normale Mandanten

Die Detailansicht besteht aus folgenden Registerkarten:

- Details**  
 Hier können Sie die Kontaktdaten und Login-Daten des Mandanten anzeigen und bearbeiten.  
 Siehe [Kapitel "Registerkarte Details", S. 17.](#)
- Extensions**  
 Hier können Sie die Extensions, die dem Mandanten zugewiesen wurden, anzeigen und verwalten.  
 Siehe [Kapitel "Registerkarte Extensions", S. 21.](#)
- PBX-Agenten-IDs**  
 Hier können Sie die PBX-Agenten-IDs, die dem Mandanten zugewiesen wurden, anzeigen und verwalten.  
 Siehe [Kapitel "Registerkarte PBX-Agenten-IDs", S. 25.](#)
- Chat-IDs**  
 Hier können Sie die Chat-IDs, die dem Mandanten zugewiesen wurden, anzeigen und verwalten.  
 Siehe [Kapitel "Registerkarte Chat-IDs", S. 28.](#)

- *Web Service*

Hier können Sie die Funktionen des Web Service aktivieren.

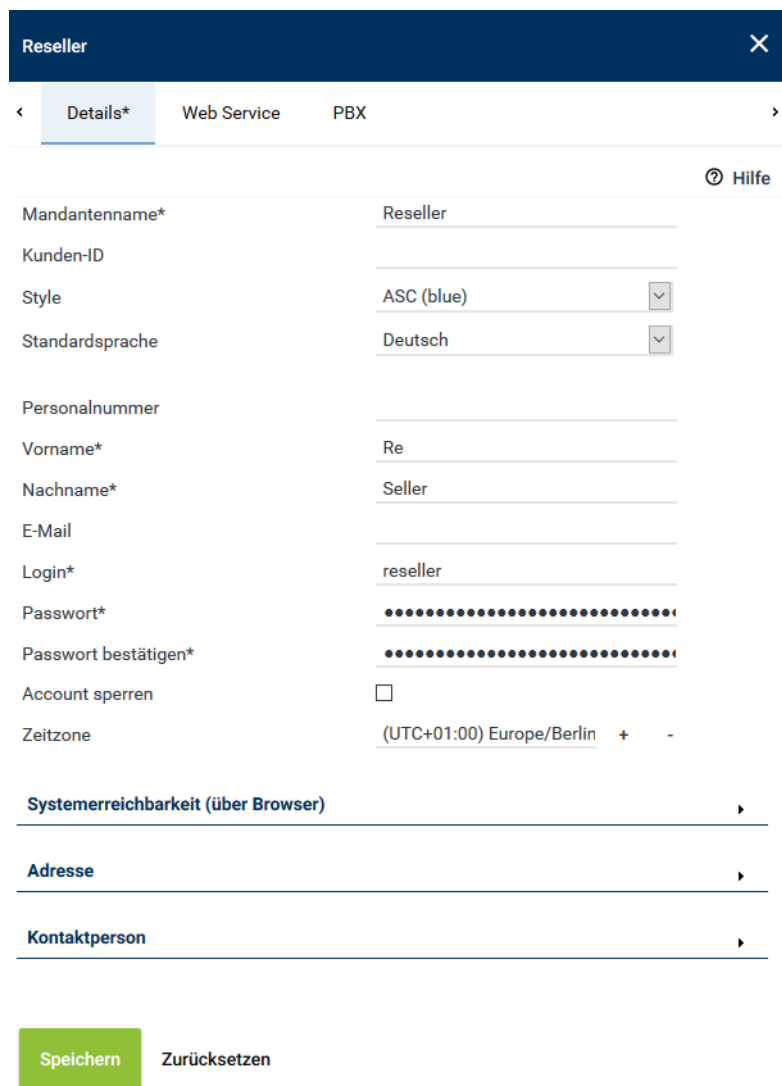
Siehe [Kapitel "Registerkarte Web Service", S. 46.](#)

- *Systemlizenzen*

Hier können Sie Module und Funktionen für Mandanten aktivieren.

Siehe [Kapitel "Registerkarte Systemlizenzen", S. 56.](#)

#### 4.2.3 Detailansicht für Wiederverkäufer



**Reseller** ✕

◀ Details\* Web Service PBX ▶

🔗 Hilfe

Mandantenname\* Reseller

Kunden-ID

Style ASC (blue) ▼

Standardsprache Deutsch ▼

Personalnummer

Vorname\* Re

Nachname\* Seller

E-Mail

Login\* reseller

Passwort\* .....

Passwort bestätigen\* .....

Account sperren ☐

Zeitzone (UTC+01:00) Europe/Berlin + -

**Systemerreichbarkeit (über Browser)** ▶

**Adresse** ▶

**Kontaktperson** ▶

**Speichern** Zurücksetzen

Abb. 5: Mandanten-Modul - Detailansicht für Wiederverkäufer

Die Detailansicht besteht aus folgenden Registerkarten:

- *Details*

Hier können Sie die Kontaktdaten und Login-Daten des Wiederverkäufers anzeigen und bearbeiten.

Siehe [Kapitel "Registerkarte Details", S. 17.](#)

- *Web Service*

Hier können Sie die Funktionen des Web Service aktivieren.

Siehe [Kapitel "Registerkarte Web Service", S. 46.](#)

- *PBX*



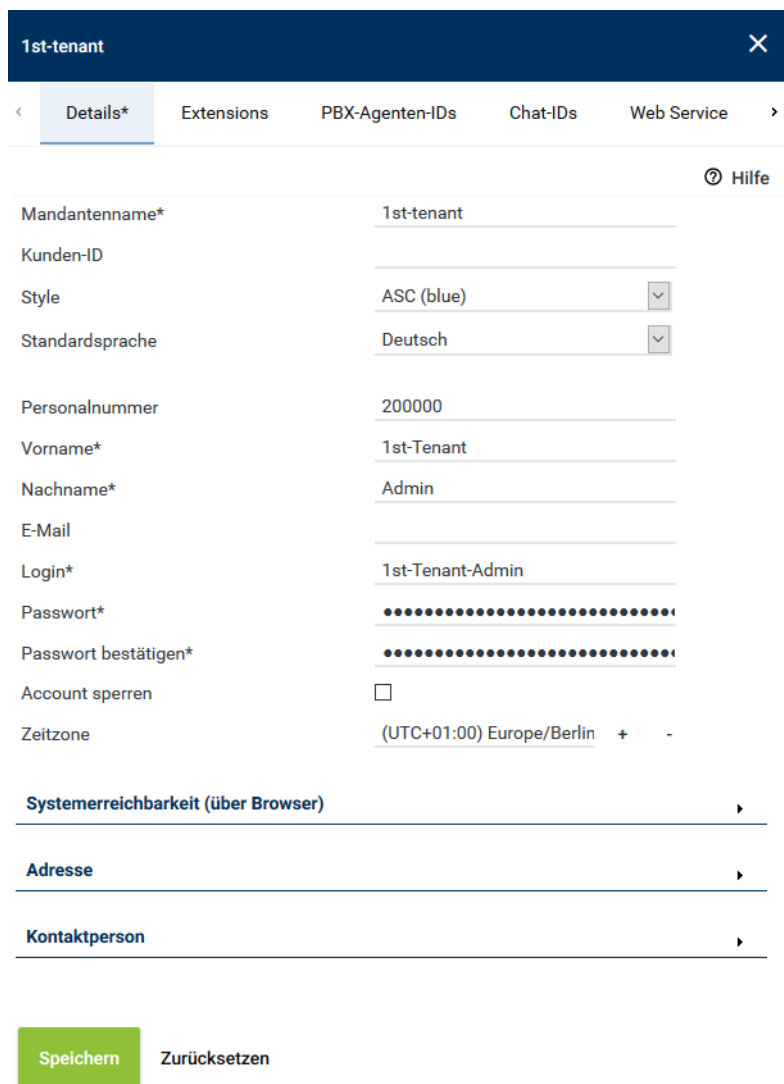
Hier können Sie [PBX-Filter](#) aktivieren und verwalten, die dem ausgewählten Mandanten zugewiesen wurden.

Siehe [Kapitel "Registerkarte PBX", S. 54](#).

#### 4.2.4 Registerkarte Details

Hier können Sie die Kontaktdaten und Login-Daten des ausgewählten Mandanten oder Wiederverkäufers anzeigen und bearbeiten.

Die Registerkarte *Details* ist für alle Mandanten oder Wiederverkäufer gleich, unabhängig davon, ob es sich um den Mandanten-Account des Systembetreibers, einen normalen Mandanten oder einen Wiederverkäufer handelt.



**1st-tenant** ✕

< Details\* Extensions PBX-Agenten-IDs Chat-IDs Web Service >

🔗 Hilfe

Mandantenname\* 1st-tenant

Kunden-ID

Style ASC (blue) ▼

Standardsprache Deutsch ▼

Personalnummer 200000

Vorname\* 1st-Tenant

Nachname\* Admin

E-Mail

Login\* 1st-Tenant-Admin

Passwort\* .....

Passwort bestätigen\* .....

Account sperren ☐

Zeitzone (UTC+01:00) Europe/Berlin + -

**Systemerreichbarkeit (über Browser)** ▶

**Adresse** ▶



**Kontaktperson** ▶

**Speichern** Zurücksetzen

Abb. 6: Mandanten-Modul - Detailansicht für normale Mandanten

- Geben Sie im allgemeinen Teil folgende Informationen ein:
  - Allgemeine Informationen zum Mandantenprofil
  - Persönliche Daten des Administrators des Mandanten
  - Login-Daten für den Administrator des Mandanten

<b>Mandantenname</b>	Name, mit dem der Mandant im System angezeigt wird.
<b>Kunden-ID</b>	Geben Sie hier die Kunden-ID ein.
<b>Style</b>	Layout, in dem die Bedienoberfläche des Systems beim Mandanten angezeigt wird.


	Wählen Sie eines der vorhandenen Layouts aus der Dropdown-Liste aus.
<i>Standardsprache</i>	Sprache, in der die Bedienoberfläche des Systems beim Mandanten angezeigt wird. Wählen Sie die Sprache aus der Dropdown-Liste aus.
<i>Personalnummer</i>	Personalnummer des Administrators des Mandanten.
<i>Vorname</i>	Vorname des Administrators des Mandanten.
<i>Nachname</i>	Nachname des Administrators des Mandanten.
<i>E-Mail</i>	E-Mail-Adresse des Administrators des Mandanten.
<i>Login</i>	Benutzername des Administrators des Mandanten.
<i>Passwort</i>	Passwort, mit dem sich der Administrator des Mandanten am System anmelden muss.
<i>Passwort bestätigen</i>	Wiederholung des Passworts für den Administrator.
<i>Account sperren</i>	Mit dieser Option können Sie den Account des Mandanten sperren. Der Mandant kann sich dann nicht mehr in <u>neo</u> anmelden. <b>HINWEIS!</b> Mit dieser Option wird nur der Account von diesem Mandanten gesperrt. Die Sperre gilt nicht für die Benutzer des Mandanten. Das heißt, die Benutzer des Mandanten können sich noch in <u>neo</u> anmelden.
<i>Zeitzone</i>	Zeigt die Zeitzone, in der die Konversationen in den Wiedergabeapplikationen angezeigt werden sollen. Diese Zeitzone wird als Voreinstellung für alle weiteren neu angelegten Angestellten gesetzt. Bei Bedarf können Sie die Zeitzone für jeden einzelnen Angestellten nachbearbeiten. Die Konfiguration im Angestellten-Modul hat höhere Priorität.  Um die Zeitzone auszuwählen, klicken Sie auf die Schaltfläche  . Siehe <a href="#">Kapitel "Zeitzone hinzufügen", S. 18</a> .  Um die Auswahl zu löschen, klicken Sie auf die Schaltfläche  .

Die Angaben in folgenden Gruppenfeldern sind optional:



- Systemerreichbarkeit (über Browser)
- Adresse
- Kontaktperson



Sobald Sie ein Gruppenfeld für optionale Angaben geöffnet haben, müssen Sie die Pflichtfelder in diesem Gruppenfeld ausfüllen, um speichern zu können. Wenn Sie die optionalen Angaben nicht machen möchten, müssen Sie das Gruppenfeld schließen, indem Sie auf das Symbol  der entsprechenden Titelleiste klicken.

#### 4.2.4.1 Zeitzone hinzufügen

1. Klicken Sie auf die Schaltfläche  rechts neben dem Eingabefeld.

Abb. 7: Zeitzone hinzufügen

2. Um die Anzeige der Tabelleneinträge zu filtern, geben Sie in das Filterfeld unterhalb der Spaltenüberschrift *Kontinent/Region* die Zeichenfolge ein, nach der gefiltert werden soll.
  - ⇒ In der Tabelle werden nur Einträge angezeigt, die in dieser Spalte die eingegebene Zeichenfolge enthalten.

Beispiel:

Sie möchten nur *Kontinente/Regionen* anzeigen, die die Zeichenfolge *ber* enthalten, also geben Sie in das Filterfeld der Spalte *Kontinent/Region* die Zeichenfolge *ber* ein:

Zeitzone	
Zeitunterschied ↕	Kontinent/Region ↕
UTC-04:00	Atlantic/Bermuda
UTC+01:00	Europe/Berlin
UTC+10:00	Australia/Canberra
<div>           Zeilen pro Seite 20 <input type="checkbox"/> 1 - 3 von 3           <span>1-4 &lt;-4 &gt;4 5-1</span> </div>	
<div>           Hinzufügen Abbrechen         </div>	

Abb. 8: Tabellenansicht nach der Zeichenfolge *ber* gefiltert (Beispiel)

3. Wählen Sie eine Zeitzone aus der Liste aus.

Zeitzone	
Zeitunterschied ↕	Kontinent/Region ↕
UTC-12:00	Etc/GMT+12
UTC-11:00	Pacific/Pago_Pago
UTC-11:00	Pacific/Samoa
UTC-11:00	Pacific/Niue
UTC-11:00	US/Samoa
UTC-11:00	Etc/GMT+11
UTC-11:00	Pacific/Midway
<div>           Zeilen pro Seite 20 <input type="checkbox"/> 1 - 20 von 616           <span>1-4 &lt;-4 &gt;4 5-1</span> </div>	
<div>           Hinzufügen Abbrechen         </div>	

Abb. 9: Zeitzone hinzufügen

4. Um die Auswahl zu übernehmen, klicken Sie auf die Schaltfläche *Hinzufügen*.  
Um die Auswahl zu verwerfen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 4.2.4.2 Gruppenfeld Systemerreichbarkeit

1. Falls Sie den Zugriff auf das System auch von außerhalb des lokalen Netzwerks ermöglichen möchten, öffnen Sie das Gruppenfeld *Systemerreichbarkeit (über Browser)*.

Systemerreichbarkeit (über Browser) ▾

+ Systemerreichbarkeit (über Browser)

Abb. 10: Systemerreichbarkeit hinzufügen

2. Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche + *Systemerreichbarkeit (über Browser)*.
3. Geben Sie die Adressen, die Sie verwenden möchten ein.

Systemerreichbarkeit (über Browser) ▾

– Systemerreichbarkeit (über Browser)

Interne IP-Adresse / Interner Port  : 443

DNS-Name

Externe IP-Adresse / Externer Port  :

Externer DNS-Name

Abb. 11: Systemerreichbarkeit konfigurieren

<i>Interne IP-Adresse / Interner Port</i>	Geben Sie hier die Ziel-IP-Adresse und den Port des Wiedergabeservers ein, unter der das Replay-Modul intern zu erreichen ist.
<i>DNS-Name</i>	Geben Sie hier den DNS-Namen ein, unter dem das Replay-Modul intern zu erreichen ist.
<i>Externe IP-Adresse / Externer Port</i>	Geben Sie die URL oder die IP-Adresse und den Port ein, unter der das Replay-Modul über den Browser auch von extern zu erreichen ist.
<i>Externer DNS-Name</i>	Geben Sie hier den externen DNS-Namen ein, unter dem das Replay-Modul über den Browser auch von extern zu erreichen ist.  <b>HINWEIS!</b> Falls das SSL-Zertifikat auf eine DNS-Adresse ausgestellt ist, muss zwingend der DNS-Name eingegeben werden, da sonst die Zertifikatsprüfung in den Wiedergabe-Applikationen fehlschlägt.



Damit die Benutzer des jeweiligen Mandanten über den Browser auf den Wiedergabeserver zugreifen können, muss im Server-Modul ebenfalls eine interne IP-Adresse bzw. auch eine externe IP-Adresse konfiguriert werden. Die Adressangaben hier und im Server-Modul müssen identisch sein.



Informationen zur Konfiguration von Servern finden Sie in der Administrationsanleitung für Systembetreiber *Konfiguration Server und Aufzeichnungsarchitekturen*.

4. Falls Sie alle Adressen entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche – *Systemerreichbarkeit (über Browser)*.

#### 4.2.4.3

#### Gruppenfeld Adresse

1. Falls Sie eine Kontaktadresse hinzufügen möchten, öffnen Sie das Gruppenfeld *Adresse*.

Adresse ▾

+ Adresse hinzufügen

Abb. 12: Adresse hinzufügen

2. Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche + *Adresse hinzufügen*.
3. Geben Sie die Adresse ein.

**Adresse** ▼

➖ Adresse entfernen

Postleitzahl

Straße

Stadt

Land

Abb. 13: Adresse hinzufügen

- Falls Sie die Adresse entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche ➖ *Adresse entfernen*.

#### 4.2.4.4 Gruppenfeld Kontaktperson

- Falls Sie eine Kontaktperson hinzufügen möchten, öffnen Sie das Gruppenfeld *Kontaktperson*.

**Kontaktperson** ▼

➕ Kontaktperson hinzufügen

Abb. 14: Kontaktperson hinzufügen

- Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche ➕ *Kontaktperson hinzufügen*.
- Geben Sie die Kontaktdaten ein.

**Kontaktperson** ▼

➖ Kontaktperson entfernen

Vorname\*

Nachname\*

E-Mail

Kommentar

Abb. 15: Kontaktperson hinzufügen



Sie können eine beliebige Kontaktperson eintragen. Die Kontaktperson muss nicht als Benutzer im System existieren.

- Falls Sie die Kontaktperson entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche ➖ *Kontaktperson entfernen*.

#### 4.2.5 Registerkarte Extensions

Hier können Sie die Extensions anzeigen und verwalten, die dem ausgewählten Mandanten zugewiesen wurden.



In 1-Mandanten-Systemen werden alle Extensions automatisch dem vom System angelegten Mandanten (1st-Tenant) zugeordnet. Die Zuordnung einer Extension zum Benutzer erfolgt im Angestellten-Modul.

Bei der Installation eines 1-Mandanten-Systems können Sie dieses Kapitel übergehen.



In Multi-Mandanten-Systemen müssen Sie jedem Mandanten die Extensions manuell zuordnen, die ihm zur Verfügung stehen sollen. Dies gilt auch für Multi-Mandanten-Systeme, in denen nur 1 Mandant angelegt ist.

Die manuelle Zuordnung der Extensions ist erst möglich, wenn eine PBX angelegt wurde, da die Zuordnung der Extensions PBX-bezogen erfolgt.

<div> <span>&lt;</span> <span>Details*</span> <span>Extensions</span> <span>PBX-Agenten-IDs</span> <span>Chat-IDs</span> <span>Web Service</span> <span>&gt;</span> </div>	
PBX	Extensions
SIP	111
SIP_	user1, user10, user2, user3, user4, user5, user6,...
<div> <span>Hinzufügen</span> <span>Verwalten</span> </div>	

Abb. 16: Mandanten-Modul - Registerkarte Extensions

- Um einem Mandanten neue Extensions zuzuweisen, gehen Sie vor wie in [Kapitel "Extensions hinzufügen", S. 22](#) beschrieben.
- Um zugewiesenen Extensions zu entfernen, gehen Sie vor wie in [Kapitel "Extensions entfernen", S. 24](#) beschrieben.
- Um eine **PBX** aus der Zuordnung zu entfernen, entfernen Sie alle zugewiesenen Extensions dieser **PBX**. Dadurch wird die Zuordnung der **PBX** gelöscht.

#### 4.2.5.1 Extensions hinzufügen

1. Markieren Sie in der Hauptansicht den Mandanten, dem Sie die Extensions zuweisen möchten.
2. Klicken Sie auf die Registerkarte *Extensions*.
3. Klicken Sie auf die Schaltfläche *Hinzufügen*.  
⇒ Das folgende Fenster erscheint:

Extensions hinzufügen ×

PBX

PBX ▼

☐ Dateiimport

☐ Datei enthält eine Überschrift

Dateiname  ...

☒ Manuelle Eingabe

Extensions oder Extension-Bereiche  
getrennt durch ";" oder "," (z. B. 3434,3535;  
4000-4100)

6000-6999

☐ Vorhandene Liste der Extensions ersetzen

Hinzufügen
Abbrechen

Abb. 17: Mandanten Extensions zuweisen

4. Wählen Sie aus der Dropdown-Liste die PBX aus, in der die Extensions für diesen Mandanten konfiguriert sind.

<b>Dateiimport</b>	<p>Wählen Sie die Option, um Extensions aus einer vorhandenen <b>CSV</b>-Datei zu importieren und der Extensions-Tabelle hinzufügen.</p> <p><b>Datei enthält eine Überschrift</b></p> <p>Aktivieren Sie die Option, damit diese Struktur beim Einlesen erkannt wird.</p> <p>Die <b>CSV</b>-Datei darf nur eine Spalte beinhalten. Werden Kommas oder andere Spalten-Trennzeichen in der <b>CSV</b>-Datei erkannt, ist die Datei nicht valide und eine Fehlermeldung erscheint.</p> <p>Als Dateiformat werden nur ZIP-Dateien unterstützt. Um eine <b>CSV</b>-Datei importieren zu können, müssen Sie diese zu einer ZIP-Datei packen.</p> <p><b>Dateiname</b></p> <p>Um einen Dateiimport vorzunehmen, gehen Sie folgendermaßen vor:</p> <ul style="list-style-type: none"> <li>Klicken Sie bei <b>Dateiname</b> auf die Schaltfläche <span style="font-size: 0.8em;">...</span>.</li> <li>Klicken Sie auf die Schaltfläche <b>Datei auswählen</b>.</li> <li>Wählen Sie über den Explorer die entsprechende ZIP-Datei aus und klicken Sie auf die Schaltfläche <b>Öffnen</b>.</li> <li>Klicken Sie auf die Schaltfläche <span style="color: #42a5f5;">➔</span> <b>Datei hochladen</b>.</li> </ul>
<b>Manuelle Eingabe</b>	<p>Wählen Sie die Option, um Extensions oder Extensions-Bereiche manuell einzugeben.</p> <p>Geben Sie den Extension-Bereich mit Bindestrich an, der für diesen Mandanten reserviert ist, z. B. von 6000 bis 6999. Alphanumerische Eingaben mit Bindestrich werden nicht als Bereich erkannt, diese müssen einzeln eingegeben werden.</p> <p>Unterschiedliche Extensions und Extensions-Bereiche können Sie durch die im Screenshot angegebenen Trennzeichen trennen.</p> <p><b>HINWEIS! Es können keine Wildcards verwendet werden!</b></p>

#### Vorhandene Liste der Extensions ersetzen

Aktivieren Sie das Kontrollkästchen, um die Liste der Extensions zu ersetzen.

☒ = Funktion ist aktiviert, die Eingabe ersetzt die Extensions der ausgewählten PBX.

☐ = Funktion ist nicht aktiviert, die konfigurierten Extensions aller PBXen werden behalten und die neuen Extensions werden zur selektierten PBX hinzugefügt.

5. Klicken Sie auf die Schaltfläche *Hinzufügen*.  
⇒ Die Extensions werden in der Extensions-Tabelle hinzugefügt.
6. Falls Fehler festgestellt wurden, erscheint das Fenster *Ergebnis*.  
Klicken Sie auf die Schaltfläche *Fehlerbericht anzeigen*, um das Fenster *Fehlerbericht* zu öffnen.  
Um das Fenster *Fehlerbericht* zu schließen, klicken Sie auf die Schaltfläche *Schließen*.  
Um das Fenster *Ergebnis* zu schließen, klicken Sie auf die Schaltfläche *Schließen*.
7. Die konfigurierten Extensions erscheinen nun in der Detailansicht.
8. Klicken Sie in der Detailansicht auf die Schaltfläche *Speichern*, um die Eingaben zu speichern.

#### 4.2.5.2 Extensions entfernen

1. Wählen Sie die Telefonanlage (PBX), für die Sie zugewiesene Extensions entfernen möchten, aus der Liste aus.

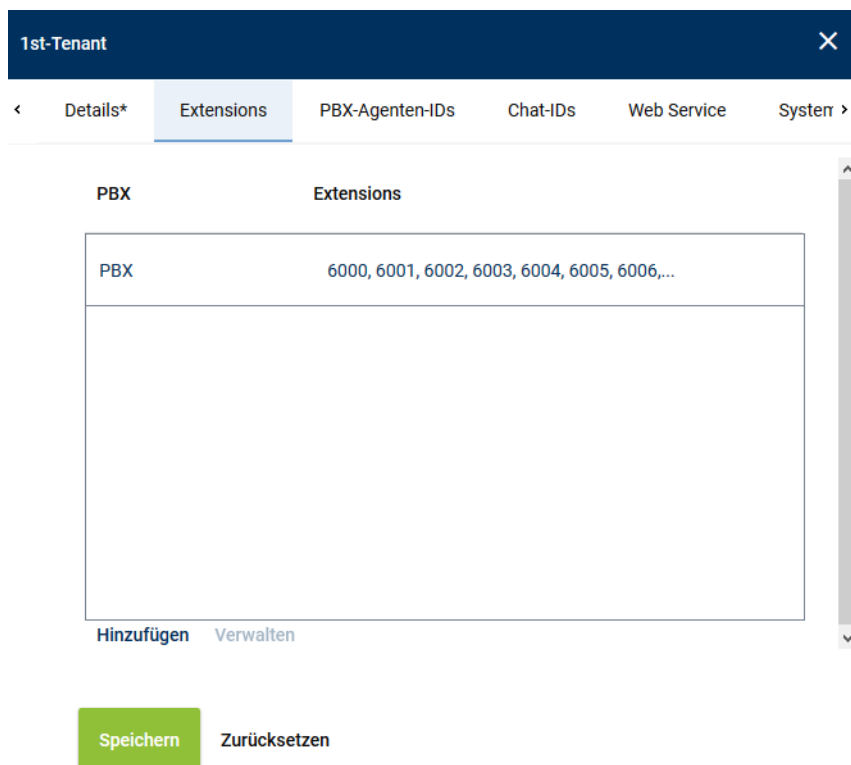


Abb. 18: Extensions entfernen

2. Klicken Sie auf die Schaltfläche *Verwalten*.
3. Wählen Sie eine oder mehrere Extensions aus, die Sie aus der Zuordnung entfernen möchten.  
Um mehrere Extensions auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.





Abb. 19: Extensions auswählen

4. Um die ausgewählten Extensions zu entfernen, klicken Sie auf die Schaltfläche *Entfernen*. Um den Vorgang abzubrechen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 4.2.6 Registerkarte PBX-Agenten-IDs

Hier können Sie die PBX-Agenten-IDs anzeigen und verwalten, die dem ausgewählten Mandanten zugewiesen wurden.



In 1-Mandanten-Systemen werden die PBX-Agenten-IDs automatisch dem vom System angelegten Mandanten (1st-Tenant) zugeordnet. Die Zuordnung einer PBX-Agenten-ID zum Benutzer erfolgt im Angestellten-Modul.

Bei der Installation eines 1-Mandanten-Systems können Sie dieses Kapitel übergehen.



In Multi-Mandanten-Systemen müssen Sie jedem Mandanten die PBX-Agenten-IDs manuell zuordnen, die ihm zur Verfügung stehen sollen. Dies gilt auch für Multi-Mandanten-Systeme, in denen nur 1 Mandant angelegt ist.

Die manuelle Zuordnung der PBX-Agenten-IDs ist erst möglich, wenn eine PBX angelegt wurde, da die Zuordnung PBX-bezogen erfolgt.



Abb. 20: Mandanten-Modul - Registerkarte PBX-Agenten-ID

- Um einem Mandanten neue PBX-Agenten-IDs zuzuweisen, gehen Sie vor wie in [Kapitel "PBX-Agenten-ID hinzufügen", S. 26](#) beschrieben.
- Um zugewiesenen PBX-Agenten-IDs zu entfernen, gehen Sie vor wie in [Kapitel "PBX-Agenten-ID entfernen", S. 28](#) beschrieben.
- Um eine [PBX](#) aus der Zuordnung zu entfernen, entfernen Sie alle zugewiesenen PBX-Agenten-IDs dieser [PBX](#). Dadurch wird die Zuordnung der [PBX](#) gelöscht.

#### 4.2.6.1 PBX-Agenten-ID hinzufügen

1. Markieren Sie in der Hauptansicht den Mandanten, dem Sie die PBX-Agenten-IDs zuweisen möchten.
2. Klicken Sie auf die Registerkarte *PBX-Agenten-IDs*.
3. Klicken Sie auf die Schaltfläche *Hinzufügen*.  
⇒ Das folgende Fenster erscheint:

PBX-Agent-IDs hinzufügen
✕

PBX

PBX
▼

☐ Dateiimport

☐ Datei enthält eine Überschrift

Dateiname  ...

☒ Manuelle Eingabe

PBX-Agent-IDs getrennt durch ";" oder ","

427agent1,427agent2

☐ Vorhandene Liste der PBX-Agent-IDs ersetzen

Hinzufügen
Abbrechen

Abb. 21: Mandanten PBX-Agenten-IDs zuweisen

4. Wählen Sie aus der Dropdown-Liste die PBX aus, in der die PBX-Agenten-IDs für diesen Mandanten konfiguriert sind.

<i>Dateiimport</i>	<p>Wählen Sie die Option, um PBX-Agenten-IDs aus einer vorhandenen <b>CSV</b>-Datei zu importieren und der PBX-Agenten-ID-Tabelle hinzuzufügen.</p> <p><b>Datei enthält eine Überschrift</b></p> <p>Aktivieren Sie die Option, damit diese Struktur beim Einlesen erkannt wird.</p> <p>Die <b>CSV</b>-Datei darf nur eine Spalte beinhalten. Werden Kommas oder andere Spalten-Trennzeichen in der <b>CSV</b>-Datei erkannt, ist die Datei nicht valide und eine Fehlermeldung erscheint.</p> <p>Als Dateiformat werden nur ZIP-Dateien unterstützt. Um eine <b>CSV</b>-Datei importieren zu können, müssen Sie diese zu einer ZIP-Datei packen.</p> <p><b>Dateiname</b></p> <p>Um einen Dateiimport vorzunehmen, gehen Sie folgendermaßen vor:</p> <ul style="list-style-type: none"> <li>• Klicken Sie bei <i>Dateiname</i> auf die Schaltfläche .</li> <li>• Klicken Sie auf die Schaltfläche <i>Datei auswählen</i>.</li> <li>• Wählen Sie über den Explorer die entsprechende ZIP-Datei aus und klicken Sie auf die Schaltfläche <i>Öffnen</i>.</li> <li>• Klicken Sie auf die Schaltfläche  <i>Datei hochladen</i>.</li> </ul>
<i>Manuelle Eingabe</i>	<p>Wählen Sie diese Option, um PBX-Agenten-IDs manuell einzugeben.</p> <p>Die einzelnen PBX-Agenten-IDs können Sie durch die im Screenshot angegebenen Trennzeichen trennen.</p> <p><b>HINWEIS! Es können keine Wildcards verwendet werden!</b></p>
<i>Vorhandene Liste der PBX-Agenten-IDs ersetzen</i>	<p>Aktivieren Sie das Kontrollkästchen, um die Liste der PBX-Agenten-IDs zu ersetzen.</p> <p><input checked="" type="checkbox"/> = Funktion ist aktiviert, die Eingabe ersetzt die PBX-Agenten-IDs der ausgewählten PBX.</p>

☐ = Funktion ist nicht aktiviert, die konfigurierten PBX-Agenten-IDs aller PBXen werden behalten und die neuen PBX-Agenten-IDs werden zur selektierten PBX hinzugefügt.

5. Klicken Sie auf die Schaltfläche *Hinzufügen*.  
⇒ Die PBX-Agenten-IDs werden in der PBX-Agenten-ID-Tabelle hinzugefügt.
6. Falls Fehler festgestellt wurden, erscheint das Fenster *Ergebnis*.  
Klicken Sie auf die Schaltfläche *Fehlerbericht anzeigen*, um das Fenster *Fehlerbericht* zu öffnen.  
Um das Fenster *Fehlerbericht* zu schließen, klicken Sie auf die Schaltfläche *Schließen*.  
Um das Fenster *Ergebnis* zu schließen, klicken Sie auf die Schaltfläche *Schließen*.
7. Die konfigurierten PBX-Agenten-IDs erscheinen nun in der Detailansicht.
8. Klicken Sie in der Detailansicht auf die Schaltfläche *Speichern*, um die Eingaben zu speichern.

#### 4.2.6.2 PBX-Agenten-ID entfernen

1. Wählen Sie die Telefonanlage (**PBX**), für die Sie zugewiesene PBX-Agenten-IDs entfernen möchten, aus der Liste aus.
2. Klicken Sie auf die Schaltfläche *Verwalten*.
3. Wählen Sie eine oder mehrere PBX-Agenten-IDs aus, die Sie aus der Zuordnung entfernen möchten.  
Um mehrere PBX-Agenten-IDs auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.



Abb. 22: PBX-Agenten-IDs auswählen

4. Um die ausgewählten PBX-Agenten-IDs zu entfernen, klicken Sie auf die Schaltfläche *Entfernen*.  
Um den Vorgang abubrechen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 4.2.7 Registerkarte Chat-IDs

Hier können Sie die Chat-IDs anzeigen und verwalten, die dem ausgewählten Mandanten zugewiesen wurden.



In 1-Mandanten-Systemen werden die Chat-IDs automatisch dem vom System angelegten Mandanten (1st-Tenant) zugeordnet. Die Zuordnung einer Chat-ID zum Benutzer erfolgt im Angestellten-Modul.

Bei der Installation eines 1-Mandanten-Systems können Sie dieses Kapitel übergehen.



In Multi-Mandanten-Systemen müssen Sie jedem Mandanten die Chat-IDs manuell zuordnen, die ihm zur Verfügung stehen sollen. Dies gilt auch für Multi-Mandanten-Systeme, in denen nur 1 Mandant angelegt ist.

Die manuelle Zuordnung der Chat-IDs ist erst möglich, wenn im PBX-Modul ein Chat-System angelegt wurde, da die Zuordnung PBX-bezogen erfolgt.

<div> <a href="#">Details*</a> <a href="#">Extensions</a> <a href="#">PBX-Agenten-IDs</a> <a href="#">Chat-IDs</a> <a href="#">Web Service</a> </div>	
Chat-System	Chat-ID
SIP	user10@ascotel2.com, user1@ascotel2.com, user2@ascotel2.com, user3@ascotel2.com, user4@ascotel2.com, user5@ascotel2.com, user6@ascotel2.com,...
<div> <a href="#">Hinzufügen</a> <a href="#">Verwalten</a> </div>	

Abb. 23: Mandanten-Modul - Registerkarte Chat-IDs

- Um einem Mandanten neue Chat-IDs zuzuweisen, gehen Sie vor wie in [Kapitel "Chat-ID hinzufügen", S. 29](#) beschrieben.
- Um zugewiesenen Chat-IDs zu entfernen, gehen Sie vor wie in [Kapitel "Chat-ID entfernen", S. 31](#) beschrieben.
- Um eine Chat-System aus der Zuordnung zu entfernen, entfernen Sie alle zugewiesenen Chat-IDs dieses Chat-Systems. Dadurch wird die Zuordnung des Chat-Systems gelöscht.

#### 4.2.7.1

#### Chat-ID hinzufügen

1. Markieren Sie in der Hauptansicht den Mandanten, dem Sie die Chat-IDs zuweisen möchten.
2. Wählen Sie die Registerkarte *Chat-IDs*.
3. Klicken Sie auf die Schaltfläche *Hinzufügen*.
  - ⇒ Das folgende Fenster erscheint:

Chat-IDs hinzufügen
✕

Chat-System Openfire

☐ Dateiimport

☐ Datei enthält eine Überschrift

Dateiname  ...

☒ Manuelle Eingabe

Chat-IDs getrennt durch \*, oder ";"



agent1@openfire2,agent2@openfire2

☐ Vorhandene Liste der Chat-IDs ersetzen

Hinzufügen
Abbrechen

Abb. 24: Mandanten Chat-IDs zuweisen

4. Wählen Sie aus der Dropdown-Liste das Chat-System aus, in dem die Chat-IDs für diesen Mandanten konfiguriert sind.

<i>Dateiimport</i>	<p>Wählen Sie die Option, um Chat-IDs aus einer vorhandenen <b>CSV</b>-Datei zu importieren und der Chat-ID-Tabelle hinzufügen.</p> <p><i>Datei enthält eine Überschrift</i></p> <p>Aktivieren Sie die Option, damit diese Struktur beim Einlesen erkannt wird.</p> <p>Die <b>CSV</b>-Datei darf nur eine Spalte beinhalten. Werden Kommas oder andere Spalten-Trennzeichen in der <b>CSV</b>-Datei erkannt, ist die Datei nicht valide und eine Fehlermeldung erscheint.</p> <p>Als Dateiformat werden nur ZIP-Dateien unterstützt. Um eine <b>CSV</b>-Datei importieren zu können, müssen Sie diese zu einer ZIP-Datei packen.</p> <p><i>Dateiname</i></p> <p>Um einen Dateiimport vorzunehmen, gehen Sie folgendermaßen vor:</p> <ul style="list-style-type: none"> <li>• Klicken Sie bei <i>Dateiname</i> auf die Schaltfläche .</li> <li>• Klicken Sie auf die Schaltfläche <i>Datei auswählen</i>.</li> <li>• Wählen Sie über den Explorer die entsprechende ZIP-Datei aus und klicken Sie auf die Schaltfläche <i>Öffnen</i>.</li> <li>• Klicken Sie auf die Schaltfläche  <i>Datei hochladen</i>.</li> </ul>
<i>Manuelle Eingabe</i>	<p>Wählen Sie diese Option, um Chat-IDs manuell einzugeben.</p> <p>Die einzelnen Chat-IDs können Sie durch die im Screenshot angegebenen Trennzeichen trennen. Die Chat-Adresse muss mit den Angaben der Agentendaten im Angestellten-Modul übereinstimmen und den Namen der entsprechenden Domäne beinhalten.</p> <p><b>HINWEIS! Es können keine Wildcards verwendet werden!</b></p>
<i>Vorhandene Liste der Chat-IDs ersetzen</i>	<p>Aktivieren Sie das Kontrollkästchen, um vorhandene Chat-IDs zu überschreiben. Falls Sie mehrere Chat-Systeme einsetzen, wird nur die Liste des selektierten Chat-Systems überschrieben.</p>

☒ = Funktion ist aktiviert, die Eingabe ersetzt die Chat-IDs des ausgewählten Chat-Systems.

☐ = Funktion ist nicht aktiviert, die konfigurierten Chat-IDs aller Chat-Systeme werden behalten und die neuen Chat-IDs werden zum selektierten Chat-System hinzugefügt.

5. Klicken Sie auf die Schaltfläche *Hinzufügen*.  
⇒ Die Chat-IDs werden in der Chat-ID-Tabelle hinzugefügt.
6. Falls Fehler festgestellt wurden, erscheint das Fenster *Ergebnis*.  
Klicken Sie auf die Schaltfläche *Fehlerbericht anzeigen*, um das Fenster *Fehlerbericht* zu öffnen.  
Um das Fenster *Fehlerbericht* zu schließen, klicken Sie auf die Schaltfläche *Schließen*.  
Um das Fenster *Ergebnis* zu schließen, klicken Sie auf die Schaltfläche *Schließen*.
7. Die konfigurierten Chat-IDs erscheinen nun in der Detailansicht.
8. Klicken Sie in der Detailansicht auf die Schaltfläche *Speichern*, um die Eingaben zu speichern.

#### 4.2.7.2 Chat-ID entfernen

1. Wählen Sie das Chat-System, für das Sie zugewiesene Chat-IDs entfernen möchten, aus der Liste aus.
2. Klicken Sie auf die Schaltfläche *Verwalten*.
3. Wählen Sie eine oder mehrere Chat-IDs aus, die Sie aus der Zuordnung entfernen möchten.  
Um mehrere Chat-IDs auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.

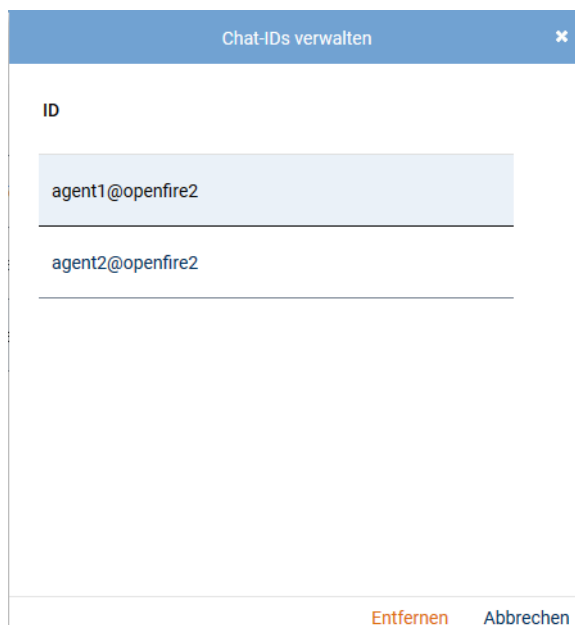


Abb. 25: Chat-IDs auswählen

4. Um die ausgewählten Chat-IDs zu entfernen, klicken Sie auf die Schaltfläche *Entfernen*.  
Um den Vorgang abubrechen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 4.2.8 Registerkarte Passwörter

Hier können Sie die Passwortregeln definieren, die von den Benutzern berücksichtigt werden müssen, wenn sie ein Passwort anlegen.

< Details*	Passwörter	Allgemeine Einstellungen*	LDAP-Verbindungsdaten*	>
<b>Passwortlänge</b> ▶				
<b>Pflichtzeichen</b> ▶				
<b>Sicherheit</b> ▶				
<b>Verbotene Passwörter</b> ▶				
<b>Erweiterte Passworteinstellungen</b> ▶				

Abb. 26: Mandanten-Modul - Registerkarte Passwörter

Die Passwortregeln werden auf alle Passwörter angewendet, die neu angelegt oder geändert werden. Bestehende Passwörter werden nicht überprüft.

Ausnahmen:

- *Gültigkeit*  
Alle Passwörter werden täglich auf die aktuell eingestellte Gültigkeitsdauer überprüft.
- *Erlaubte Anzahl von fehlgeschlagenen Logins*  
Für alle Passwörter wird bei jedem Login-Versuch die Anzahl der fehlerhaften Eingaben überwacht.

In folgende Fällen werden die definierten Passwortregeln **nicht** angewendet:


- Authentifizierung erfolgt via [LDAP](#)
- Der Benutzer ist Superuser
- Im Account des Benutzers ist folgende Option aktiviert:  
*Passwortregeln müssen nicht erfüllt werden*

Parameter, die den Wert 0 oder keinen Wert enthalten, werden ignoriert.




Die Definition von Passwortregeln ist optional.



Sobald Sie ein Gruppenfeld für optionale Angaben geöffnet haben, müssen Sie die Pflichtfelder in diesem Gruppenfeld ausfüllen, um speichern zu können. Wenn Sie die optionalen Angaben nicht machen möchten, müssen Sie das Gruppenfeld schließen, indem Sie auf das Symbol  der entsprechenden Titelleiste klicken.

### Gruppenfeld Passwortlänge

1. Um Passwortlängen festzulegen, öffnen Sie das Gruppenfeld *Passwortlänge*.
2. Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Passwortlänge*. Wertebereich für alle Eingabefelder: 0 bis 256
3. Geben Sie im Feld *Minimale Länge*, die Anzahl von Zeichen ein, die ein Passwort mindestens haben muss.



**Passwortlänge** ▼

➖ Passwortlänge entfernen

Minimale Länge (max. 3 Zeichen)	<u>1</u>
Maximale Länge (max. 3 Zeichen)	<u>256</u>

Abb. 27: Passwortlänge festlegen

- Geben Sie im Feld *Maximale Länge*, die Anzahl von Zeichen ein, die ein Passwort höchstens haben darf.

**HINWEIS!** *Maximale Länge* muss  $\geq$  *Minimale Länge* sein.

- Falls Sie die Eingaben entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche ➖ *Passwortlänge entfernen*.

### Gruppenfeld Pflichtzeichen

- Um Pflichtzeichen festzulegen, öffnen Sie das Gruppenfeld *Pflichtzeichen*.
- Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche ➕ *Pflichtzeichen*.
- Füllen Sie alle oder nur einzelne Felder aus:  
Wertebereich für alle Eingabefelder: 0 bis 256

**Pflichtzeichen** ▼

➖ Pflichtzeichen entfernen

Max. Zeichenwiederholung (max. 3 Zeichen)	<u>256</u>
Min. Anzahl von Buchstaben (max. 3 Zeichen)	<u>2</u>
Ziffern (max. 3 Zeichen)	<u>2</u>
Satzzeichen (max. 3 Zeichen)	<u>1</u>
Kleinbuchstaben (max. 3 Zeichen)	<u>0</u>
Großbuchstaben (max. 3 Zeichen)	<u>0</u>


Abb. 28: Pflichtzeichen festlegen

Max. Zeichenwiederholung	Geben Sie ein, wie oft ein Zeichen direkt aufeinander folgend wiederholt werden darf.		
	Beispiele:		
	Max. Zeichenwiederholung	Gültig	Ungültig
	0	abc	aabc
	1	aabcabc	aaabcabc
	2	aaabc	aaaabcabc
Min. Anzahl von Buchstaben	Geben Sie ein, wie viele Buchstaben das Passwort mindestens enthalten muss.		
Min. Anzahl von Zahlen	Geben Sie ein, wie viele Zahlen das Passwort mindestens enthalten muss.		
Min. Anzahl von Satzzeichen	Geben Sie ein, wie viele Satzzeichen das Passwort mindestens enthalten muss.		


	Gültige Satzzeichen:
	Punkt .
	Komma ,
	Semikolon ;
	Doppelpunkt :
	Fragezeichen ?
	Ausrufezeichen !
	Anführungszeichen ""
	Apostroph '
	Bindestrich -
	Schrägstrich /
	Klammern ( ) [ ] { }
	Alle anderen Satzzeichen werden als Buchstaben interpretiert.
<i>Kleinbuchstaben</i>	Geben Sie ein, wie viele Kleinbuchstaben das Passwort mindestens enthalten muss.
<i>Großbuchstaben</i>	Geben Sie ein, wie viele Großbuchstaben das Passwort mindestens enthalten muss.

4. Falls Sie die Eingaben entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Pflichtzeichen entfernen*.

### Gruppenfeld Sicherheit

- Um Einstellungen zur Sicherheit vorzunehmen, öffnen Sie das Gruppenfeld *Sicherheit*.
- Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Sicherheit*.
- Füllen Sie alle oder nur einzelne Felder aus:  
Wertebereich für alle Eingabefelder: 0 bis 999

**Sicherheit** ▼

 *Sicherheit entfernen*

Gültigkeit  
(max. 3 Zeichen)  Tag(e)

Informationszeitpunkt über baldigen  
Passwortablauf  
(max. 3 Zeichen)  Tag(e)

Passworthistorie

☒ Passworthistorie in Tagen  
 Tag(e)

☐ Größe der Passworthistorie


Erlaubte Anzahl von fehlgeschlagenen  
Logins  
(max. 3 Zeichen)

Private Daten nicht erlauben ☐


Abb. 29: Passwortsicherheit konfigurieren

<i>Gültigkeit</i>	Geben Sie ein, wie lange ein Passwort gültig bleibt. <i>Gültigkeit = 0</i> : Passwörter laufen nie ab
<i>Informationszeitpunkt über baldigen Passwortablauf</i>	Geben Sie ein, wie viele Tage vor Ablauf der Passwort-Gültigkeit der Benutzer darüber informiert werden soll, dass er sein Passwort bald ändern muss.

	<p><i>Informationszeitpunkt ... = 0: Benutzer wird nicht informiert</i></p> <p><b>HINWEIS!</b> Der Wert für den Informationszeitpunkt muss kleiner sein als der Wert für die Gültigkeit des Passworts.</p>
<i>Passworthistorie</i>	<p>Geben Sie ein, wie lange die Passworthistorie gespeichert werden soll. Wählen Sie zwischen folgenden Optionen:</p> <ul style="list-style-type: none"> <li>• <i>Passworthistorie in Tagen</i> Geben Sie für diese Option ein, wie lange die Passwörter in der Passworthistorie gespeichert werden sollen.</li> <li>• <i>Größe der Passworthistorie</i> Geben Sie für diese Option die Anzahl der Passwörter ein, die in der Passworthistorie gespeichert werden sollen.</li> </ul> <p>Die Passworthistorie wird in beiden Fällen nie komplett gelöscht. Wenn der eingestellte Wert erreicht wird, werden lediglich die ältesten Einträge gelöscht.</p>
<i>Erlaubte Anzahl von fehlgeschlagenen Logins</i>	<p>Geben Sie ein, wie oft der Benutzer maximal ein falsches Passwort eingeben darf, bevor sein Account gesperrt wird.</p> <p><b>HINWEIS!</b> Ein gesperrter Account kann von jedem Benutzer wieder freigegeben werden, der Zugriff auf das Angestellten-Modul und auf die Daten des gesperrten Benutzers hat.</p>
<i>Private Daten nicht erlauben</i>	<p>Stellen Sie ein, ob der Benutzer in seinem Passwort private Daten aus seinem Profil verwenden darf (z. B. Name, Benutzername, Geburtstag).</p> <p><input checked="" type="checkbox"/> = Private Daten sind nicht erlaubt.</p> <p><input type="checkbox"/> = Private Daten sind erlaubt.</p>

4. Falls Sie die Eingaben entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Sicherheit entfernen*.

### Gruppenfeld Verbotene Passwörter

- Um verbotene Passwörter festzulegen, öffnen Sie das Gruppenfeld *Verbotene Passwörter*.
- Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Verbotene Passwörter*.
- Stellen Sie in der Liste *Verbotene Passwörter* alle Wörter zusammen, die nicht als Passwort verwendet werden dürfen.



**HINWEIS!** Groß- und Kleinschreibung wird nicht unterschieden.

**Verbotene Passwörter** ▼

 *Verbotene Passwörter entfernen*

Verwende Blacklist für Passwörter ☒


**Verbotene Passwörter**

Server	
System	

**Hinzufügen** **Löschen**

Abb. 30: Verbotene Passwörter festlegen

**Hinzufügen** Fügt einen neuen Eintrag zur Liste hinzu.

<b>Löschen</b>	Löscht den ausgewählten Eintrag aus der Liste.
	Öffnet den ausgewählten Eintrag zur Bearbeitung (siehe <a href="#">Kapitel "Eintrag bearbeiten", S. 36</a> ).

- Wenn Sie die Überwachung auf die eingegebenen Wörter aktivieren möchten, aktivieren Sie das Kontrollkästchen hinter *Verwende Blacklist für Passwörter*.

<i>Verwende Blacklist für Passwörter</i>	<input checked="" type="checkbox"/> = Überwachung ist aktiviert. <input type="checkbox"/> = Überwachung ist deaktiviert. Die Angaben in der Liste werden ignoriert.
--	--

- Falls Sie die Eingaben entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Verbotene Passwörter entfernen*.

### Gruppenfeld Erweiterte Passworteinstellungen


- Um erweiterte Passworteinstellungen festzulegen, öffnen Sie das Gruppenfeld *Erweiterte Passworteinstellungen*.
- Stellen Sie ein, ob die Passwortregeln ignoriert werden dürfen.




<b>Erweiterte Passworteinstellungen</b>	▼
Passwortregeln können ignoriert werden	<input type="checkbox"/>

Abb. 31: Erweiterte Passworteinstellungen festlegen

<i>Passwortregeln können ignoriert werden</i>	<input checked="" type="checkbox"/> = Passwortregeln können ignoriert werden. Um die Passwortregeln bei einem Benutzer zu ignorieren, aktivieren Sie zusätzlich im Account des Benutzers die Option <i>Passwortregeln müssen nicht erfüllt werden</i> . <input type="checkbox"/> = Passwortregeln können nicht ignoriert werden.
---	--



#### 4.2.8.1 Eintrag bearbeiten

- Um einen Listeneintrag anzupassen, klicken Sie in der entsprechenden Zeile auf das Symbol  (*Bearbeiten*).  
 ⇒ Der Eintrag wird in einem Eingabefeld editiert.

0002100010000	
0602150016666	
New value	 

Hinzufügen Löschen

Abb. 32: Listeneintrag bearbeiten

- Passen Sie den Eintrag an.
- Um die Änderungen zu speichern, klicken Sie auf das Symbol  (*Speichern*).  
 Um die Änderungen zu verwerfen, klicken Sie auf das Symbol  (*Verwerfen*).

#### 4.2.9 Registerkarte Allgemeine Einstellungen

Hier können Sie verschiedene allgemeine Einstellungen vornehmen.

< Details\*    Passwörter    **Allgemeine Einstellungen\***    LDAP-Verbindungsdati >

---

**Inaktivität** ▶

---

**SMTP-Account** ▶

---

**SNMP-Agent** ▶

---

**Login-Einstellungen** ▶

---

**Sonstige Einstellungen** ▶

---

**Nutzungsbedingungen** ▶

---

Abb. 33: Mandanten-Modul - Registerkarte Allgemeine Einstellungen

#### 4.2.9.1 Gruppenfeld Inaktivität

**Inaktivität** ▼

---

Vor Sperrung benachrichtigen\*  
(max. 3 Zeichen)  0 Tag(e)


Benutzer wird inaktiv gesetzt\*  
(max. 3 Zeichen)  0 Tag(e)

Session-Timeout

☒ Session-Timeout  
 30 Minute(n)

☐ Session läuft nie ab

Abb. 34: Benutzerinaktivität konfigurieren

<i>Vor Sperrung benachrichtigen</i>	<p>Stellen Sie ein, wie viele Tage vor Sperrung des Accounts ein Benutzer darüber benachrichtigt wird, dass sein Account gesperrt werden wird. Der Benutzer wird gesperrt, wenn er die im Feld <i>Benutzer wird inaktiv gesetzt</i> eingestellte Anzahl an Tagen inaktiv war.</p> <p>Die Benachrichtigung erfolgt an die E-Mail-Adresse des Benutzers.</p>
<i>Benutzer wird inaktiv gesetzt</i>	<p>Stellen Sie ein, nach wie vielen Tagen der Inaktivität der Account des Benutzers gesperrt wird.</p>
<i>Session-Timeout</i>	<p>Stellen Sie ein, nach wie vielen Minuten der Inaktivität die Sitzung des Benutzers automatisch beendet werden soll. Wählen Sie zwischen folgenden Optionen:</p> <ul style="list-style-type: none"> <li>• <i>Session-Timeout</i> Diese Option aktiviert den Session-Timeout. Geben Sie einen Wert von 5 bis 1440 ein.</li> <li>• <i>Session läuft nie ab</i> Diese Option deaktiviert den Session-Timeout und erlaubt Endlos-Sessions.</li> </ul> <p><b>HINWEIS!</b> Bei dieser Option ist folgendes zu beachten: Falls der Benutzer die Applikation nicht korrekt über die Logoff-Funktion (Menüpunkt  (<i>Angemeldet als</i>) &gt; <i>Logoff</i>) beendet und den Browser einfach schließt, wird die gestartete</p>


Session nie beendet. Jede endlose Session belegt Speicher. Dies kann unter Umständen dazu führen, dass der Server neu gestartet werden muss. Bei einem Neustart des Servers werden alle Sessions beendet.




Änderungen an diesen Einstellungen werden bei den verschiedenen Benutzern erst nach einer neuen Anmeldung am System wirksam.

#### 4.2.9.2 Gruppenfeld SMTP-Account

Um die Funktion des E-Mail-Versandes für Systemnachrichten nutzen zu können, müssen Sie in der Applikation System Configuration den **SMTP-Account** des System-Benutzers konfigurieren.

1. Um einen **SMTP-Account** hinzuzufügen, öffnen Sie das Gruppenfeld *SMTP-Account*.
2. Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *SMTP-Account*.


**SMTP-Account** ▼

 SMTP-Account entfernen

TLS aktivieren	<input type="checkbox"/>
SMTP-Timeout	<input type="text" value="10"/> Sek
SMTP-Port	<input type="text" value="25"/>
Absender*	<input type="text"/>
SMTP-Server*	<input type="text"/>
Login	<input type="text"/>
Passwort	<input type="text"/>

Abb. 35: SMTP-Account hinzufügen




Sobald Sie ein Gruppenfeld für optionale Angaben geöffnet haben, müssen Sie die Pflichtfelder in diesem Gruppenfeld ausfüllen, um speichern zu können. Wenn Sie die optionalen Angaben nicht machen möchten, müssen Sie das Gruppenfeld schließen, indem Sie auf das Symbol  der entsprechenden Titelleiste klicken.

3. Füllen Sie folgende Felder aus:

<i>TLS aktivieren</i>	Stellen Sie ein, ob Sie das Verschlüsselungsprotokoll <b>TLS</b> aktivieren möchten. <input checked="" type="checkbox"/> = <b>TLS</b> ist aktiviert. <input type="checkbox"/> = <b>TLS</b> ist deaktiviert.
<i>SMTP-Timeout</i>	Geben Sie hier ein, nach wie vielen Sekunden eine Timeout-Meldung erfolgen soll, falls keine Verbindung zum SMTP-Server aufgebaut werden kann.
<i>SMTP-Port</i>	Geben Sie hier den Port ein, über den das Login erfolgen soll. Default-Wert: 25 (TLS: 587)
<i>Absender</i>	Geben Sie hier die E-Mail-Adresse ein, die in den versendeten E-Mails als Absenderadresse eingetragen werden soll.
<i>SMTP-Server</i>	Geben Sie hier die <b>IP</b> -Adresse oder den Namen des <b>SMTP</b> -Servers ein, auf dem der Account eingerichtet ist.
<i>Login</i>	Geben Sie hier den Login-Namen für die Authentifizierung am <b>SMTP</b> -Server ein.

**Passwort** Geben Sie hier das Passwort für die Authentifizierung am [SMTP-Server](#) ein.

- Falls Sie den SMTP-Account entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  **SMTP-Account entfernen**.

#### 4.2.9.3 Gruppenfeld SNMP-Agent

Damit das Aufzeichnungssystem [SNMP-GET](#)-Anfragen von externen Überwachungsprogrammen bedienen kann, müssen Sie hier einen [SNMP](#)-Agenten konfigurieren.



Als *Community Name* muss in den [SNMP-GET](#)-Anfragen der Wert *public* verwendet werden.



Für [SNMP-GET](#)-Anfragen nutzt das Aufzeichnungssystem einen systemeigenen [SNMP](#)-Dienst. Der [SNMP](#)-Dienst des Betriebssystems wird **nicht** genutzt.

Bitte deaktivieren Sie den [SNMP](#)-Dienst des Betriebssystems, falls Sie ihn für keine anderen Anwendungen benötigen!


Per [SNMP-GET](#) kann der Systemstatus abgefragt werden. Mögliche Ergebnisse einer Systemstatus-Abfrage sind:

OK	Das System funktioniert fehlerfrei.
ERROR	Mindestens ein überwachtes Objekt ist ausgefallen. Im Feld <i>DESCRIPTION</i> der <a href="#">SNMP</a> -Antwort werden alle ausgefallenen Objekte werden aufgelistet.  <b>HINWEIS!</b> Detaillierte Informationen zum Fehler eines Objekts können Sie im Status-Modul der Applikation System Monitoring einsehen, siehe Bedienungsanleitung <i>System Monitoring</i> .

Alle [SNMP](#)-Objekte des Aufzeichnungssystems sind in folgender [MIB](#)-Datei definiert:

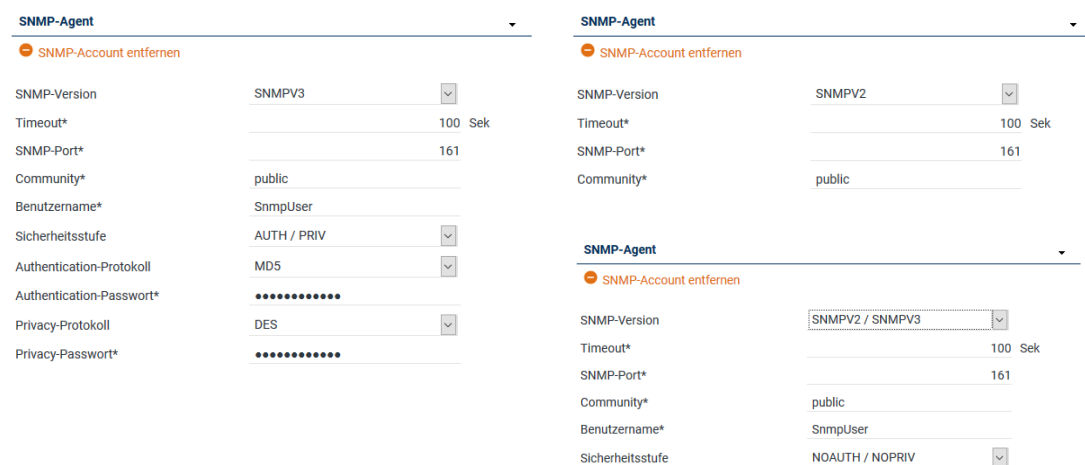
- C:\Program Files (x86)\ASC\ASC Product Suite\data\mib\ASC-SNMP-MIB-NEO.txt

#### SNMP-Agent einrichten

- Um die Funktion einzurichten, öffnen Sie das Gruppenfeld *SNMP-Agent*.
- Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  **SNMP-Agent**.



Welche Eingabefelder angezeigt werden, ist abhängig davon, welche [SNMP](#)-Version und welche Sicherheitsstufe Sie wählen.



The screenshot shows two instances of the 'SNMP-Agent' configuration form. The left instance shows the configuration for SNMPV3, and the right instance shows the configuration for SNMPV2. Both forms include fields for Timeout, Port, Community, Username, Security Level, Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password. The right instance also shows a dropdown for the SNMP Version (SNMPV2 / SNMPV3) and a dropdown for the Security Level (NOAUTH / NOPRIV).


Abb. 36: Gruppenfeld SNMP-Agent (Beispiele)

- Füllen Sie alle erforderlichen Felder aus:


<i>SNMP-Version</i>	<p>Wählen Sie aus der Dropdown-Liste die <b>SNMP</b>-Version aus, die Sie verwenden möchten.</p> <p>Folgende Versionen stehen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <i>SNMPV2</i></li> <li>• <i>SNMPV2 / SNMPV3</i></li> <li>• <i>SNMPV3</i></li> </ul>
<i>Timeout</i>	<p>Geben Sie hier ein, nach wie vielen Sekunden eine Timeout-Meldung erfolgen soll, falls keine Verbindung zum <b>SNMP</b>-Server aufgebaut werden konnte.</p>
<i>SNMP-Port</i>	<p>Geben Sie hier den Port ein, über den die <b>SNMP</b>-Anfragen eingehen sollen. Default-Wert: <i>161</i></p> <p><b>HINWEIS!</b> Falls auch der <b>SNMP</b>-Dienst des Betriebssystems genutzt wird, können Sie den Default-Port <b>nicht</b> verwenden. Tragen Sie in diesem Fall einen anderen Port ein.</p>
<i>Benutzername</i>	<p>(Nur für <b>SNMP</b>-Versionen <i>SNMPV2/SNMPV3</i> und <i>SNMPV3</i>.)</p> <p>Definieren Sie hier den Benutzernamen, der für <b>SNMP</b>-Anfragen verwendet werden muss.</p>
<i>Sicherheitsstufe</i>	<p>(Nur für <b>SNMP</b>-Versionen <i>SNMPV2/SNMPV3</i> und <i>SNMPV3</i>.)</p> <p>Wählen Sie aus der Dropdown-Liste die Sicherheitsstufe aus, die Sie verwenden möchten.</p> <p>Folgende Sicherheitsstufen stehen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <i>NOAUTH / NOPRIV</i> <p>Das externe <b>SNMP</b>-Programm muss sich nicht authentifizieren.</p> <p>Die <b>SNMP</b>-Antwort wird unverschlüsselt übertragen.</p> </li> <li>• <i>AUTH / NOPRIV</i> <p>Wählen Sie diese Option, wenn Sie möchten, dass sich das externe <b>SNMP</b>-Programm authentifizieren muss, die <b>SNMP</b>-Antwort aber unverschlüsselt übertragen wird.</p> <p>Wählen Sie in diesem Fall im Feld <i>Authentication-Protokoll</i> einen Protokolltypen aus und geben Sie im Feld <i>Authentication-Passwort</i> ein zugehöriges Passwort ein.</p> </li> <li>• <i>AUTH / PRIV</i> <p>Wählen Sie diese Option, wenn Sie möchten, dass sich das externe <b>SNMP</b>-Programm authentifizieren muss und die <b>SNMP</b>-Antwort verschlüsselt übertragen wird.</p> <p>Wählen Sie in diesem Fall im Feld <i>Authentication-Protokoll</i> einen Protokolltypen aus und geben Sie im Feld <i>Authentication-Passwort</i> ein zugehöriges Passwort ein.</p> <p>Wählen Sie außerdem im Feld <i>Privacy-Protokoll</i> einen Protokolltypen aus und geben Sie im Feld <i>Privacy-Passwort</i> ein zugehöriges Passwort ein.</p> </li> </ul>
<i>Authentication-Protokoll</i>	<p>(Nur für Sicherheitsstufen <i>AUTH / NOPRIV</i> und <i>AUTH / PRIV</i>.)</p> <p>Wählen Sie hier das Protokoll aus, das Sie für die Authentifizierung des externen <b>SNMP</b>-Programms verwenden möchten.</p> <p>Folgende Protokolltypen stehen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <i>MD5</i></li> <li>• <i>SHA</i></li> </ul>



<b>Authentication-Passwort</b>	(Nur für Sicherheitsstufen <i>AUTH / NOPRIV</i> und <i>AUTH / PRIV</i> .) Geben Sie hier ein Passwort für die Authentifizierung ein. Passwortlänge: 8 bis 15 Zeichen
<b>Privacy-Protokoll</b>	(Nur für Sicherheitsstufe <i>AUTH / PRIV</i> .) Wählen Sie hier das Protokoll aus, das Sie für die Verschlüsselung der <b>SNMP</b> -Antwort verwenden möchten. Folgende Protokolltypen stehen zur Verfügung: <ul style="list-style-type: none"> <li>• <i>DES</i></li> <li>• <i>AES-128</i></li> </ul>
<b>Privacy-Passwort</b>	(Nur für Sicherheitsstufe <i>AUTH / PRIV</i> .) Geben Sie hier ein Passwort für die Verschlüsselung der <b>SNMP</b> -Antwort ein. Passwortlänge: 8 bis 15 Zeichen

4. Falls Sie den SMTP-Account entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  **SNMP-Account entfernen**.




Sobald Sie ein Gruppenfeld für optionale Angaben geöffnet haben, müssen Sie die Pflichtfelder in diesem Gruppenfeld ausfüllen, um speichern zu können. Wenn Sie die optionalen Angaben nicht machen möchten, müssen Sie das Gruppenfeld schließen, indem Sie auf das Symbol  der entsprechenden Titelleiste klicken.



**SNMP**-Trap-Nachrichten können Sie im Nachrichten-Modul konfigurieren, siehe Administrationsanleitung *System Configuration - Nachrichten-Modul*.

#### 4.2.9.4

#### Gruppenfeld Login-Einstellungen

**Login-Einstellungen**


---

SSO-Login aktivieren	<input type="checkbox"/>
JWT-Login aktivieren	<input type="checkbox"/>
OAuth-Login aktivieren	<input checked="" type="checkbox"/>
OAuth-API-Endpunkt	<input type="text"/>
OAuth-Client-ID	<input type="text"/>
Alternative Login-Fehler-Seite	<input checked="" type="radio"/> Keine <input type="radio"/> Standard <input type="radio"/> Benutzerdefiniert
	<input type="text"/>
LDAP-Login aktivieren	<input type="checkbox"/>

Abb. 37: Login-Einstellungen konfigurieren

<b>SSO-Login aktivieren</b>	<p>Hier können Sie für die Benutzer des Aufzeichnungssystems <b>SSO</b>-Login aktivieren bzw. deaktivieren.</p> <p>Aktivieren bzw. deaktivieren Sie das Login per Single Sign On (<b>SSO</b>).</p> <p><input checked="" type="checkbox"/> = <b>SSO</b>-Login ist aktiviert  <input type="checkbox"/> = <b>SSO</b>-Login ist nicht aktiviert</p> <p>Sobald Sie die Funktion hier aktiviert haben, können alle Benutzer aller Mandanten <b>SSO</b> nutzen. Die einzelnen Mandanten müssen keine weiteren Konfigurationen vornehmen.</p> <p><b>Einzige weitere Voraussetzung</b> für die Nutzung von <b>SSO</b>:</p>
-----------------------------	---

	<ul style="list-style-type: none"> <li>Damit sich ein Benutzer per <b>SSO</b> am System anmelden kann, muss sein Benutzername im Aufzeichnungssystem (siehe Angeestellten-Modul, Registerkarte <i>Account</i>) mit dem Windows-Benutzernamen übereinstimmen und die Domain enthalten. Format: <i>Domain\Windows-Benutzername</i></li> </ul> <p><b>HINWEIS!</b> Das Benutzerpasswort im Aufzeichnungssystem muss <b>nicht</b> mit dem Passwort des Windows-Accounts übereinstimmen. Bei einem <b>SSO</b>-Login wird nur das Benutzerpasswort ausgewertet. Das Windows-Passwort wird ignoriert.</p> <p><b>HINWEIS!</b> Wenn Sie sowohl <b>SSO</b>-Login als auch <b>LDAP</b>-Login aktivieren, werden die LDAP-Daten ignoriert, wenn sich der Benutzer mit seinem Windows-Account anmeldet.</p> <p><b>Einschränkungen</b> bei der Nutzung von <b>SSO</b>:</p> <ul style="list-style-type: none"> <li>Kombinations-Login nicht möglich</li> <li>In der Adressleiste des Browsers muss zwingend die IP-Adresse des Applikationsservers verwendet werden. Die Verwendung eines DNS-Namens ist nicht möglich.</li> </ul>
<i>JWT-Login aktivieren</i>	<p>Hier können Sie für die Benutzer des Aufzeichnungssystems die Authentifizierung per JWT-Login aktivieren bzw. deaktivieren.</p> <p>Aktivieren bzw. deaktivieren Sie die Authentifizierung per JWT.</p> <p><input checked="" type="checkbox"/> = ist aktiviert <input type="checkbox"/> = ist nicht aktiviert</p> <p>JWT-Login ist ein spezielles Login-Verfahren, bei dem die Applikation von externer Seite einen Token (JWT-Token) mit bestimmten Identifikations-Attributen erhält und diese dann verifiziert. Sind die Information im Token gültig, wird der Benutzer ohne weitere Passwortprüfung oder ähnliches in das System eingeloggt. Sind die Informationen im Token ungültig, wird dem Benutzer der Zugang versperrt.</p> <p><b>HINWEIS!</b> Um die Gültigkeit der externen Tokens überprüfen zu können, muss ein gültiges Zertifikat des externen Systems in <i>neo</i> importiert werden.</p>
<i>OAuth-Login aktivieren</i>	<p>Hier können Sie für die Benutzer des Aufzeichnungssystems die Authentifizierung per OAuth-Login aktivieren bzw. deaktivieren.</p> <p>Aktivieren bzw. deaktivieren Sie die Authentifizierung per OAuth.</p> <p><input checked="" type="checkbox"/> = ist aktiviert <input type="checkbox"/> = ist nicht aktiviert</p>
<i>OAuth-API-Endpunkt</i>	<p>Hier können Sie den OAuth-API-Endpunkt eingeben (z. B. <a href="https://authentication.example.org.token">https://authentication.example.org.token</a>).</p>
<i>OAuth-Client-ID</i>	<p>Hier können Sie die OAuth-Client-ID eingeben (z. B. ef0129223a2e3bf76e7c3d8422b15b).</p>
<i>Alternative Login-Fehler-Seite</i>	<p>Hier können Sie die Anzeige einer alternativen Login-Fehler-Seite im Falle eines ungültigen Logins aktivieren.</p> <p>Aktivieren Sie die Anzeige der alternativen Login-Fehler-Seite.</p> <ul style="list-style-type: none"> <li><i>Keine</i> Diese Option aktiviert keine Login-Fehler-Seite. Im Falle eines Login-Fehlers erscheint im Anmeldebildschirm eine Fehlermeldung. Nach Schließen der Fehlermeldung kann ein erneuter Login ausgeführt werden.</li> </ul>

- *Standard*

Diese Option aktiviert die Standard Login-Fehler-Seite.

Im Falle eines Login-Fehlers wird eine neue Seite angezeigt. Auf dieser Seite wird beschrieben, dass der Login fehlgeschlagen ist und der Benutzer den Administrator kontaktieren soll.

- *Benutzerdefiniert*

Diese Option aktiviert eine benutzerdefinierte Login-Fehler-Seite. Geben Sie im Eingabefeld die entsprechende Web-Adresse ein (z. B. [www.Beispiel-Login-Fehler.de](http://www.Beispiel-Login-Fehler.de)).

Im Falle eines Login-Fehlers wird zur hier angegebene Web-Adresse verbunden.

#### LDAP-Login aktivieren

Hier können Sie für die Benutzer ihres Bereichs die Authentifizierung per [LDAP](#) grundsätzlich aktivieren bzw. deaktivieren.

Aktivieren bzw. deaktivieren Sie die Authentifizierung per [LDAP](#).

☒ = [LDAP](#)-Login ist aktiviert

☐ = [LDAP](#)-Login ist nicht aktiviert

**HINWEIS!** Wenn Sie sowohl [SSO](#)-Login als auch [LDAP](#)-Login aktivieren, werden die LDAP-Daten ignoriert, wenn sich der Benutzer mit seinem Windows-Account anmeldet.

**HINWEIS!** [LDAP](#)-Login kann erst aktiviert werden, wenn Sie mindestens 1 [LDAP](#)-Verbindung konfiguriert haben (siehe [Kapitel "Registerkarte LDAP-Verbindungsdaten"](#), S. 44).

#### 4.2.9.5

#### Gruppenfeld Sonstige Einstellungen

**Sonstige Einstellungen** ▼

---

☒ Letztes Login-Datum anzeigen

☒ Logout-Warnung anzeigen

☒ Resource-String-Ansicht

☒ Fehlgeschlagene Anmeldung


☐ Logoff-Funktion deaktivieren

☐ Passwort vergessen ausblenden

System-Ankündigung

Abb. 38: Sonstige Einstellungen konfigurieren

<b>Letztes Login-Datum anzeigen</b>	Stellen Sie ein, ob Sie das letzte Login-Datum in allen Applikationen anzeigen möchten. <input checked="" type="checkbox"/> = Anzeige ist aktiviert <input type="checkbox"/> = Anzeige ist nicht aktiviert
<b>Logout-Warnung anzeigen</b>	Stellen Sie ein, ob Sie eine Logout-Warnung in allen Applikationen anzeigen möchten. <input checked="" type="checkbox"/> = Anzeige ist aktiviert <input type="checkbox"/> = Anzeige ist nicht aktiviert
<b>Resource-String-Ansicht</b>	Stellen Sie ein, ob Sie eine Resource-String-Ansicht in allen Applikationen anzeigen möchten.

	<input checked="" type="checkbox"/> = Anzeige ist aktiviert <input type="checkbox"/> = Anzeige ist nicht aktiviert
<i>Fehlgeschlagene Anmeldung</i>	Stellen Sie ein, ob Sie eine fehlgeschlagene Anmeldung in allen Applikationen anzeigen möchten.  <input checked="" type="checkbox"/> = Anzeige ist aktiviert <input type="checkbox"/> = Anzeige ist nicht aktiviert
<i>Logoff-Funktion deaktivieren</i>	Stellen Sie ein, ob Sie die Logoff-Funktion (Menüpunkt  (Angemeldet als) > Logoff) anzeigen möchten.  <input checked="" type="checkbox"/> = Logoff-Funktion wird nicht angezeigt <input type="checkbox"/> = Logoff-Funktion wird angezeigt
<i>Passwort vergessen ausblenden</i>	Stellen Sie ein, ob Sie die Funktion <i>Passwort vergessen?</i> in den Login-Fenstern anzeigen möchten.  <input checked="" type="checkbox"/> = Funktion <i>Passwort vergessen?</i> wird nicht angezeigt <input type="checkbox"/> = Funktion <i>Passwort vergessen?</i> wird angezeigt
<i>System-Ankündigung</i>	Hier können Sie eine Mitteilung (Wartungsankündigung) an die Mandanten verfassen.  Die Mitteilung wird im Browser-Anmeldebildschirm der <i>neo</i> -Applikation angezeigt.

#### 4.2.9.6 Gruppenfeld Nutzungsbedingungen

**Nutzungsbedingungen** ▼

Nutzungsbedingungen  
(max. 4000 Zeichen)

Abb. 39: Nutzungsbedingungen konfigurieren

<i>Nutzungsbedingungen</i>	Hier können Sie die Nutzungsbedingungen eingeben.  Die Nutzungsbedingungen werden nach dem Login der <i>neo</i> -Applikation im Browser angezeigt und müssen mit <i>OK</i> bestätigt werden.
----------------------------	--

#### 4.2.10 Registerkarte LDAP-Verbindungsdaten

Hier können Sie die **LDAP**-Verbindungsdaten verwalten. Wenn Sie mehrere **LDAP**-Verbindungen anlegen, durchsucht das System bei einem Login-Versuch per **LDAP** so lange alle Verbindungskonfigurationen bis eine der Verbindungen erfolgreich ist.

Die Nutzung der **LDAP**-Authentifizierung können Sie in der Registerkarte *Allgemeine Einstellungen* aktivieren (siehe [Kapitel "Gruppenfeld Login-Einstellungen"](#), S. 41).



Abb. 40: Mandanten-Modul - Registerkarte LDAP-Authentifizierung

<b>Hinzufügen</b>	Öffnet ein Fenster, in dem Sie eine neue <b>LDAP</b> -Verbindung hinzufügen können (siehe <a href="#">Kapitel "LDAP-Verbindungsdaten bearbeiten"</a> , S. 45).
<b>Bearbeiten</b>	Öffnet den ausgewählten Eintrag zur Bearbeitung (siehe <a href="#">Kapitel "LDAP-Verbindungsdaten bearbeiten"</a> , S. 45).
<b>Löschen</b>	Löscht den ausgewählten Eintrag aus der Liste.

#### 4.2.10.1 LDAP-Verbindungsdaten bearbeiten

Serveradresse	Port
159.159.159.159.	6611
123.123.123.123	4711

Hinzufügen   Bearbeiten   Löschen

Abb. 41: LDAP-Verbindungsdaten

- Um eine neue **LDAP**-Verbindung zu konfigurieren, klicken Sie auf die Schaltfläche *Hinzufügen*.  
Um eine bestehende **LDAP**-Verbindung zu bearbeiten, klicken Sie auf die Schaltfläche *Bearbeiten*.



Abb. 42: LDAP-Verbindungsdaten bearbeiten (Beispiel)

<b>Serveradresse</b>	IP-Adresse des <b>LDAP</b> -Servers.
<b>Port</b>	Port am <b>LDAP</b> -Server, über den die Verbindung aufgebaut werden soll.

	Im Standard wird folgender Port verwendet: 389 = <b>LDAP</b> -Verbindung, unverschlüsselt 636 = <b>LDAP</b> -Verbindung, verschlüsselt
<b>SSL verwenden</b>	Aktivieren bzw. deaktivieren Sie die Verwendung des <b>SSL</b> -Protokolls. <input checked="" type="checkbox"/> = <b>SSL</b> wird verwendet <input type="checkbox"/> = <b>SSL</b> wird nicht verwendet <b>HINWEIS!</b> <b>SSL</b> kann nur verwendet werden, wenn der <b>LDAP</b> -Server <b>SSL</b> unterstützt.
<b>DN des Benutzers</b>	Distinguished Name (DN) des Benutzers für die Authentifizierung am <b>LDAP</b> -Server.
<b>Passwort</b>	Passwort für die Authentifizierung am <b>LDAP</b> -Server.

2. Füllen Sie alle Felder oder nur die Pflichtfelder aus.
3. Um zu kontrollieren, ob mit den eingegebenen Daten eine Verbindung zum **LDAP**-Server aufgebaut werden kann, klicken Sie auf die Schaltfläche *LDAP-Verbindung prüfen*.  
⇒ Das Ergebnis der Prüfung wird im Fenster *Verbindungsdaten bearbeiten* angezeigt.
4. Um die Eingaben zu speichern und in die Liste zu übernehmen, klicken Sie auf die Schaltfläche *OK*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 4.2.11 Registerkarte Web Service

Die *neo*-Software bietet eine Schnittstelle für die Durchführung von Funktionen per Web Service.

In dieser Registerkarte können Sie einstellen, welche der grundsätzlich für Web Service zur Verfügung gestellten Funktionen in Ihrem Aufzeichnungssystem genutzt werden dürfen. Die Freigabe der einzelnen Funktionen erfolgt für jeden Mandanten individuell. Welche Funktionen grundsätzlich zur Verfügung stehen und in der Registerkarte angezeigt werden, ist abhängig davon, ob Sie in der Hauptansicht einen Mandanten-Account oder den Systembetreiber-Account ausgewählt haben.

##### 4.2.11.1 Web Service für den Systembetreiber konfigurieren

Hier können Sie die Funktionen des Web Service aktivieren oder deaktivieren, die der Systembetreiber nutzen können soll.

1. Wählen Sie in der Hauptansicht den Account des Systembetreibers aus.
2. Wählen Sie die Registerkarte *Web Service*.

< Allgemeine Einstellungen\*
LDAP-Verbindungsdaten\*
Web Service
>

**Allgemeine Funktionen**

☒ Testet die grundlegende Web-Service-Funktionalität

**Angestellte**

☐ Erlaubt den Export von Funktionsrechten  
☐ Erlaubt den Import von Rollen  
☐ Erlaubt den Export von Rollen

**Mandant**

☒ Erlaubt den Export von Mandanteninformationen  
☒ Erlaubt den Export der Extension-Zuordnung  
☒ Erlaubt die Zuordnung und Administration von Extensions  
☒ Erlaubt das Löschen eines Mandanten  
☒ Erlaubt das Ändern einer Extension  
☐ Erlaubt das Zurückziehen von Vormetric-Schlüsseln  
☒ Erlaubt den Import von neuen und bereits existierenden Mandanten

**Konfiguration**

☒ Erlaubt das Importieren von Monitorpunkten  
☒ Erlaubt den Import von Telefonen  
☐ Erlaubt den Export von Telefonen  
☐ Erlaubt den Export von Monitorpunkten

Abb. 43: Web-Service-Funktionen für den Systembetreiber

3. Aktivieren Sie die Kontrollkästchen der Funktionen, die aktiviert werden sollen.
  - ☒ = Funktion ist aktiviert
  - ☐ = Funktion ist nicht aktiviert

### Gruppenfeld Allgemeine Funktionen

In diesem Gruppenfeld können Sie die Testfunktion aktivieren.

<i>Testet die grundlegende Web-Service-Funktionalität</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie den Test der allgemeinen Web-Service-Funktionalität zulassen möchten.
---	---

### Gruppenfeld Angestellte

In diesem Gruppenfeld können Sie die Funktionen zur Verwaltung der Angestellten konfigurieren.

<i>Erlaubt den Export von Funktionsrechten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Funktionsrechte exportieren kann.
<i>Erlaubt den Import von Rollen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Rollen importieren kann.
<i>Erlaubt den Export von Rollen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Rollen exportieren kann.

### Gruppenfeld Mandant

In diesem Gruppenfeld können Sie die Funktionen zur Verwaltung der Mandanten konfigurieren.



<i>Erlaubt den Export von Mandanteninformationen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie über den Web Service Mandanteninformationen exportieren können.  Mandanteninformationen sind z. B. Mandantenname, die verwendete Standardsprache, Personalnummer, Vorname, Nachname oder die E-Mail-Adresse.
<i>Erlaubt den Export der Extension-Zuordnung</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie die zugewiesenen Extensions eines Mandanten über den Web Service exportieren können.
<i>Erlaubt die Zuordnung und Administration von Extensions</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie den Mandanten über den Web Service Extensions zuordnen können.
<i>Erlaubt das Löschen eines Mandanten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service einen Mandanten löschen kann.
<i>Erlaubt das Ändern einer Extension</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service eine Extension ändern kann.
<i>Erlaubt das Zurückziehen von Vormetric-Schlüsseln</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service die Vormetric-Schlüsselverwaltung zurückziehen kann.
<i>Erlaubt den Import von neuen und bereits existierenden Mandanten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie über den Web Service Mandanten hinzufügen und Daten von bestehenden Mandanten überschreiben können.

### Gruppenfeld Konfiguration

In diesem Gruppenfeld können Sie die Funktionen zur Konfiguration der Mandanten konfigurieren.

<i>Erlaubt das Importieren von Monitorpunkten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Monitorpunkte importieren kann.
<i>Erlaubt den Import von Telefonen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Telefone importieren kann.
<i>Erlaubt den Export von Telefonen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Telefone exportieren kann.
<i>Erlaubt den Export von Monitorpunkten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Monitorpunkte importieren kann.

#### 4.2.11.2 Web Service für den Mandanten konfigurieren

Hier können Sie die Funktionen des Web Service aktivieren oder deaktivieren, die der Mandant nutzen können soll.

1. Wählen Sie in der Hauptansicht den Account des Mandanten aus, für den Sie die Einstellungen vornehmen möchten.
2. Wählen Sie die Registerkarte *Web Service*.



Abb. 44: Web-Service-Funktionen für den Mandanten

- |  |   |
|--|---|
| <i>Erlaubt den Export von Funktionsrechten</i>                             | Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Funktionsrechte exportieren kann.   |
| <i>Erlaubt den Import von neuen und bereits existierenden Angestellten</i> | Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Angestellte hinzufügen und die Daten bestehender Angestellten überschreiben kann. |
| <i>Erlaubt den Import von Rollen</i>                                       | Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Rollen importieren kann.  |
| <i>Erlaubt den Export von Rollen</i>                                       | Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Rollen exportieren kann.  |

<i>Erlaubt den Export von Angestellten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Angestellte exportieren kann.
--	---

### Gruppenfeld Konversation

In diesem Gruppenfeld können Sie die Funktionen für die Suche und den Export von Konversationen über den Web Service konfigurieren.

<i>Erlaubt den Export von Konversationen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Konversationen exportieren kann.  <b>HINWEIS!</b> Wenn Sie diese Funktion aktivieren, müssen Sie im Gruppenfeld <i>Konversationen Exportserver</i> eine Exportserver eintragen.
<i>Erlaubt die Suche von Konversationen über Web Service</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Konversationen suchen kann.
<i>Erlaubt den Export von Transkriptionen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Transkriptionen exportieren kann.
<i>Löschzeit für Konversationen setzen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service eine Löschzeit für Konversationen setzen kann.
<i>Löschzeit für Pakete setzen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service eine Löschzeit für Pakete setzen kann.

### Gruppenfeld Mandant

In diesem Gruppenfeld können Sie die Funktionen zur Verwaltung der Mandanten konfigurieren.

<i>Erlaubt den Export von Organisationseinheiten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Organisationseinheiten exportieren kann.
<i>Erlaubt das Zurückziehen von Vormetric-Schlüsseln</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service die Vormetric-Schlüsselverwaltung zurückziehen kann.
<i>Erlaubt das Importieren von Organisationseinheiten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Organisationseinheiten importieren kann.

### Gruppenfeld Konversationen Exportserver

In diesem Gruppenfeld können Sie den Exportserver konfigurieren, auf dem die Konversationen liegen, die über den Web Service exportiert werden sollen.

<i>Exportserver</i>	Klicken Sie rechts neben dem Feld <i>Exportserver</i> auf die Schaltfläche <b>+</b> .
---------------------	---

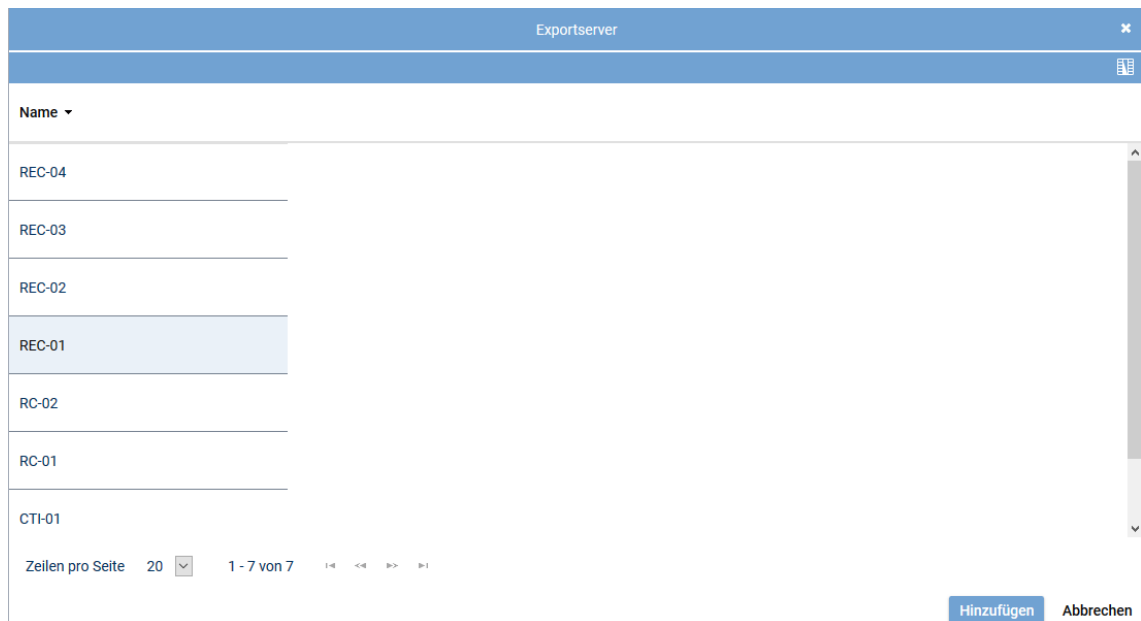


Abb. 45: Exportserver auswählen

**HINWEIS!** Für einen Exportserver muss zwingend die Eigenschaft *Wiedergabe* aktiviert sein. Deshalb werden in der Liste nur Server angezeigt, die als Wiedergabeserver konfiguriert sind.

1. Wählen Sie aus der Liste den Server aus, von dem die Konversationen exportiert werden sollen.
2. Klicken Sie auf die Schaltfläche *Hinzufügen*.  
⇒ Der Name des Exportservers erscheint in der Detailansicht.



Informationen zur Konfiguration von Servern und Aufzeichnungsarchitekturen finden Sie in der Administrationsanleitung für Systembetreiber *Konfiguration Server und Aufzeichnungsarchitekturen*.

#### 4.2.11.2.1 Server zuordnen

1. Klicken Sie hinter dem Eingabefeld *Exportserver* auf die Schaltfläche **+**.

\_\_\_\_\_ + -

Abb. 46: Server zuordnen

2. Wählen Sie den passenden Server aus der Liste aus.



Abb. 47: Server auswählen (Beispiel)

- Um den ausgewählten Server zu übernehmen, klicken Sie auf die Schaltfläche *Hinzufügen*. Um die Auswahl zu verwerfen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 4.2.11.3 Pfad der WSDL-Datei

In der mitgelieferten [WSDL](#)-Datei sind die Funktionen aufgelistet, die mit dem Web Service genutzt werden können.

Geben Sie folgende URL im Browser ein: <http://<Rekorder-IP>/ASCWebService/ASCWebServiceService?wsdl>, um die [WSDL](#)-Datei aufzurufen.

#### Rückgabewerte

- Import:  
Wenn ein Import ausgeführt wird, erscheint im System Monitoring im Jobs-Modul in der Spalte *Job-Status* ein Eintrag über den Erfolg bzw. Misserfolg.
- Export:  
Der Export kann an den ausgelesenen Daten geprüft werden, dem boolschen Wert über den Erfolg bzw. Misserfolg sowie an der Fehlerbeschreibung bei einem Misserfolg.

#### 4.2.11.4 Web Service für den Wiederverkäufer konfigurieren

Hier können Sie die Funktionen des Web Service aktivieren oder deaktivieren, die der Wiederverkäufer nutzen können soll.

- Wählen Sie in der Hauptansicht den Account des Wiederverkäufers aus.
- Wählen Sie die Registerkarte *Web Service*.

< Details\*
Web Service
PBX >

**Allgemeine Funktionen**

☐ Testet die grundlegende Web-Service-Funktionalität

**Angestellte**

☐ Erlaubt den Export von Funktionsrechten  
☐ Erlaubt den Import von Rollen  
☐ Erlaubt den Export von Rollen

**Mandant**

☐ Erlaubt den Export von Mandanteninformationen  
☐ Erlaubt den Export der Extension-Zuordnung  
☐ Erlaubt die Zuordnung und Administration von Extensions  
☐ Erlaubt das Löschen eines Mandanten  
☐ Erlaubt das Ändern einer Extension  
☐ Erlaubt das Zurückziehen von Vormetric-Schlüsseln  
☐ Erlaubt den Import von neuen und bereits existierenden Mandanten

**Konfiguration**

☐ Erlaubt das Importieren von Monitorpunkten  
☐ Erlaubt den Import von Telefonen  
☐ Erlaubt den Export von Telefonen  
☐ Erlaubt den Export von Monitorpunkten

Abb. 48: Web-Service-Funktionen für den Wiederverkäufer

3. Aktivieren Sie die Kontrollkästchen der Funktionen, die aktiviert werden sollen.  
☒ = Funktion ist aktiviert  
☐ = Funktion ist nicht aktiviert

### Gruppenfeld Allgemeine Funktionen

In diesem Gruppenfeld können Sie die Testfunktion aktivieren.

<i>Testet die grundlegende Web-Service-Funktionalität</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie den Test der allgemeinen Web-Service-Funktionalität zulassen möchten.
---	---

### Gruppenfeld Angestellte

In diesem Gruppenfeld können Sie die Funktionen zur Verwaltung der Angestellten konfigurieren.

<i>Erlaubt den Export von Funktionsrechten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Funktionsrechte exportieren kann.
<i>Erlaubt den Import von Rollen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Rollen importieren kann.
<i>Erlaubt den Export von Rollen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Rollen exportieren kann.

### Gruppenfeld Mandant

In diesem Gruppenfeld können Sie die Funktionen zur Verwaltung der Mandanten konfigurieren.

<i>Erlaubt den Export von Mandanteninformationen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie über den Web Service Mandanteninformationen exportieren können.  Mandanteninformationen sind z. B. Mandantenname, die verwendete Standardsprache, Personalnummer, Vorname, Nachname oder die E-Mail-Adresse.
<i>Erlaubt den Export der Extension-Zuordnung</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie die zugewiesenen Extensions eines Mandanten über den Web Service exportieren können.
<i>Erlaubt die Zuordnung und Administration von Extensions</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie den Mandanten über den Web Service Extensions zuordnen können.
<i>Erlaubt das Löschen eines Mandanten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie den Mandanten über den Web Service löschen können.
<i>Erlaubt das Ändern einer Extension</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie die Extension über den Web Service ändern können.
<i>Erlaubt das Zurückziehen von Vormetric-Schlüsseln</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service die Vormetric-Schlüsselverwaltung zurückziehen kann.
<i>Erlaubt den Import von neuen und bereits existierenden Mandanten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass Sie über den Web Service Mandanten hinzufügen und Daten von bestehenden Mandanten überschreiben können.

### Gruppenfeld Konfiguration

In diesem Gruppenfeld können Sie die Funktionen zur Konfiguration der Mandanten konfigurieren.

<i>Erlaubt das Importieren von Monitorpunkten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Monitorpunkte importieren kann.
<i>Erlaubt den Import von Telefonen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Telefone importieren kann.
<i>Erlaubt den Export von Telefonen</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Telefone exportieren kann.
<i>Erlaubt den Export von Monitorpunkten</i>	Aktivieren Sie das Kontrollkästchen, wenn Sie zulassen möchten, dass der Mandant über den Web Service Monitorpunkte importieren kann.

#### 4.2.12 Registerkarte PBX

Hier können Sie [PBX](#)-Filter aktivieren und verwalten, die dem ausgewählten Mandanten zugewiesen wurden.

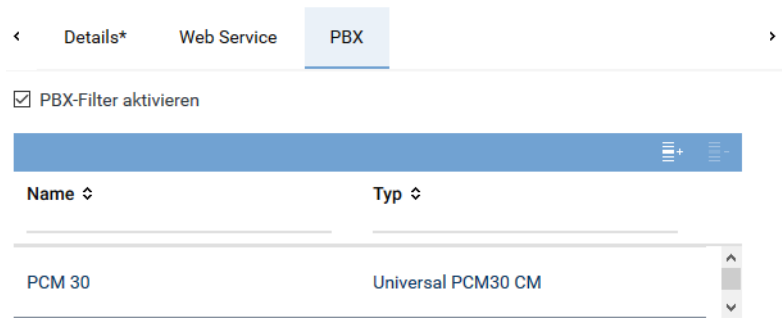



Abb. 49: Mandanten-Modul - Registerkarte PBX

**PBX-Filter aktivieren** Aktivieren Sie das Kontrollkästchen, wenn Sie dem Wiederverkäufer nur Zugriff auf zugewiesene **PBX**en erlauben möchten.

- Um einem Wiederverkäufer eine **PBX** zuzuweisen, gehen Sie vor wie in [Kapitel "PBX zuweisen"](#), S. 55 beschrieben.
- Um eine **PBX**-Zuweisung für den Wiederverkäufer zu entfernen, gehen Sie vor wie in [Kapitel "PBX-Zuweisung entfernen"](#), S. 56 beschrieben.

#### 4.2.12.1 PBX zuweisen

1. Klicken Sie auf das Symbol  (*Hinzufügen*).

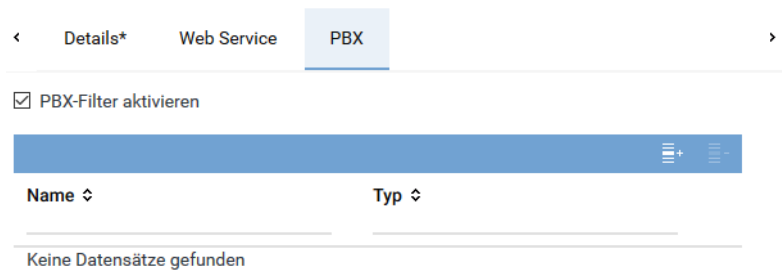


Abb. 50: PBX zuweisen

2. Wählen Sie eine **PBX** aus der Liste aus.  
Um mehrere **PBX**en auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.



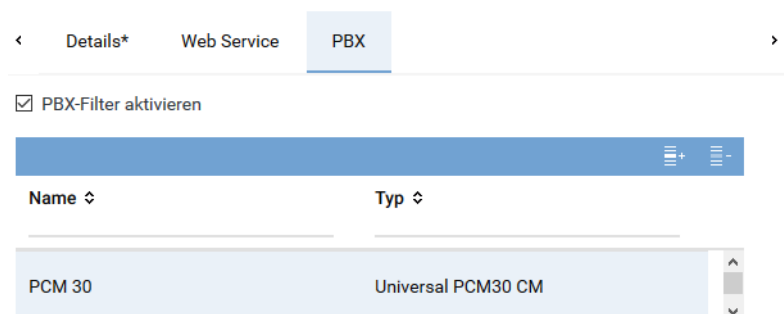
Name	Typ
AL	ALCATEL OmniPCX
Universal Import	Universal Import
Alcatel OmniPCX	ALCATEL OmniPCX
PCM 30	Universal PCM30 CM
PRI passive DP	Universal PRI passive DP
MVTC	Universal MVTC

Abb. 51: PBX hinzufügen

- Klicken Sie auf die Schaltfläche *Hinzufügen*.  
Um die Auswahl zu verwerfen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 4.2.12.2 PBX-Zuweisung entfernen

- Wählen Sie eine **PBX** aus der Liste aus.  
Um mehrere **PBX**en auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.



Name	Typ
PCM 30	Universal PCM30 CM

Abb. 52: PCX-Zuweisung entfernen

- Klicken Sie auf das Symbol  (*Entfernen*).

#### 4.2.13 Registerkarte Systemlizenzen



Die Registerkarte wird nur angezeigt, wenn eine Lizenz vom Typ *Cloud Recording* im System vorhanden ist.

Hier können Sie Module und Funktionen für Mandanten aktivieren.



<
Details\*
Web Service
Systemlizenzen
>

---

**Systemlizenzen**
▼

---

☐ Nachkomprimierung
   
☒ Agenten-Modul
   
☒ Zuweisungen-Modul
   
☒ E-Learning
   
☒ Export von Konversationen

**Compliance-Lizenzen**
▼

---

☐ Compliance-Modus

Abb. 53: Registerkarte Systemlizenzen

### Gruppenfeld Systemlizenzen

<b>Nachkomprimierung</b>	<p>Stellen Sie ein, ob die aufgezeichneten Konversationen komprimiert werden sollen.</p> <p><input checked="" type="checkbox"/> = Aufzeichnungen werden komprimiert.</p> <p><input type="checkbox"/> = Aufzeichnungen werden nicht komprimiert.</p> <p><b>HINWEIS!</b> Um die Nachkomprimierung nutzen zu können, benötigen Sie pro Kanal, der komprimiert werden soll, 1 Lizenz vom Typ <i>Data Compression</i>.</p> <p>Durch die Komprimierung der gespeicherten Konversationen ist es möglich, die Anzahl der speicherbaren Aufzeichnungen zu erhöhen. Außerdem wird die notwendige Netzwerkbandbreite für eine eventuelle Übertragung der Aufzeichnungsdaten verringert.</p> <p>Zur Komprimierung der Aufzeichnungen wird der standardisierte Algorithmus <a href="#">G.729A</a> verwendet. <a href="#">G.729A</a> komprimiert Audiodaten bei Stereo-Gesprächen von 128 Kbit/s auf eine Datenrate von 16 Kbit/s, bei Mono-Gesprächen von 64 Kbit/s auf 8 Kbit/s. Voraussetzung für die Anwendung der Nachkomprimierung ist, dass die Konversationen im G.711- oder G.722-Format (A-law oder <math>\mu</math>-law) vorliegen.</p> <p><b>HINWEIS!</b> Ist die Komprimierung aktiviert, erfolgt die Übertragung auf die Speichererweiterung erst, nachdem die Komprimierung erfolgt ist. Eine Komprimierungsverzögerung verzögert also auch die Übertragung auf die Speichererweiterung.</p> <p><b>HINWEIS!</b> Daten, die bereits komprimiert wurden, werden bei einer eventuellen Datenübertragung nicht wieder dekomprimiert, selbst wenn für das Ziellaufwerk keine Komprimierung eingestellt ist. D. h. weder bei der Übertragung komprimierter Daten zwischen verschiedenen Systemspeichern noch bei der Übertragung von einem Systemspeicher auf seine Speichererweiterung erfolgt eine Dekomprimierung.</p> <p><b>HINWEIS!</b> Aufzeichnungen werden ab dem Zeitpunkt der Aktivierung der Nachkomprimierung komprimiert. Aufzeichnungen, die bereits auf die Speichererweiterung übertragen wurden, werden <b>nicht</b> nachträglich komprimiert.</p>
--------------------------	--

	<b>HINWEIS!</b> Die Laufwerke müssen für die Nachkomprimierung konfiguriert sein. Weitere Informationen finden Sie in der Administrationsanleitung <i>System Configuration - Konfiguration Laufwerke</i> . Die Nachkomprimierung gilt für alle Laufwerke, für die die Nachkomprimierung aktiviert ist.
<i>Agenten-Modul</i>	Stellen Sie ein, ob das Agenten-Modul aktiviert werden soll. <input checked="" type="checkbox"/> = Agenten-Modul ist aktiviert. <input type="checkbox"/> = Agenten-Modul ist nicht aktiviert.
<i>Zuweisungen-Modul</i>	Stellen Sie ein, ob das Zuweisungen-Modul aktiviert werden soll. <input checked="" type="checkbox"/> = Zuweisungen-Modul ist aktiviert. <input type="checkbox"/> = Zuweisungen-Modul ist nicht aktiviert.
<i>E-Learning</i>	Stellen Sie ein, ob das E-Learning-Modul aktiviert werden soll. <input checked="" type="checkbox"/> = E-Learning-Modul ist aktiviert. <input type="checkbox"/> = E-Learning-Modul ist nicht aktiviert.
<i>Export von Konversationen</i>	Stellen Sie ein, ob der Export von Konversationen aktiviert werden soll. <input checked="" type="checkbox"/> = Export von Konversationen ist aktiviert. <input type="checkbox"/> = Export von Konversationen ist nicht aktiviert.

### Gruppenfeld Compliance-Lizenzen



Dieses Gruppenfeld wird nur angezeigt, wenn die Lizenz *INSPIRATION for Compliance* im System vorhanden ist.

<i>Compliance-Modus</i>	Stellen Sie ein, ob der Compliance-Modus für INSPIRATION <sup>neo</sup> aktiviert werden soll. <input checked="" type="checkbox"/> = Compliance-Modus ist aktiviert. <input type="checkbox"/> = Compliance-Modus ist nicht aktiviert.
-------------------------	---


### 4.3

#### Neuen Mandanten manuell anlegen

1. Wählen Sie in der Hauptansicht den Systembetreiber oder Wiederverkäufer aus, unter dem Sie einen Mandanten oder Wiederverkäufer anlegen möchten.

+ × Mandanten Allgemein ▾	
Name	Typ
▾ System	Systembetreiber
1st-tenant	Mandant
2nd-Tenant	Mandant
3rd-Tenant	Mandant

Abb. 54: Mandanten-Modul - Hauptansicht (Beispiel)

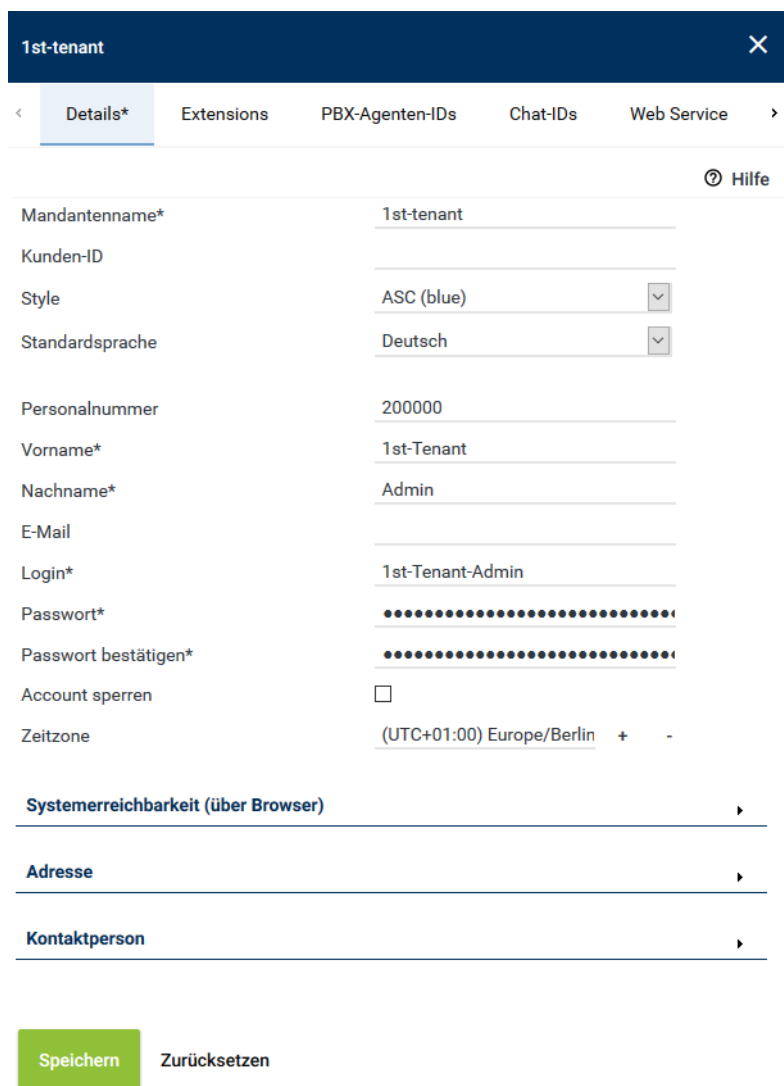
2. Klicken Sie in der Symbolleiste auf das Symbol  (*Hinzufügen*).
3. Wählen Sie eine der folgenden Optionen:

<b>Mandant erstellen</b>	Ein neuer Mandant wird erstellt.
--------------------------	----------------------------------

**Wiederverkäufer erstellen**

Ein neuer Wiederverkäufer wird erstellt.

- Nehmen Sie in der Detailansicht alle notwendigen Einstellungen in den Registerkarten vor. Sie können dabei ohne Zwischenspeicherung zwischen den Registerkarten wechseln, ohne dass Ihre Einstellungen verloren gehen.
- Um nach der Beendigung der Eingaben die Einstellungen zu speichern, klicken Sie auf die Schaltfläche *Speichern*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Zurücksetzen*.



**1st-tenant** [X]

< Details\* Extensions PBX-Agenten-IDs Chat-IDs Web Service >

ⓘ Hilfe

Mandantenname\* 1st-tenant

Kunden-ID

Style ASC (blue) [v]

Standardsprache Deutsch [v]

Personalnummer 200000

Vorname\* 1st-Tenant

Nachname\* Admin

E-Mail

Login\* 1st-Tenant-Admin

Passwort\* .....

Passwort bestätigen\* .....

Account sperren ☐

Zeitzone (UTC+01:00) Europe/Berlin + -

**Systemerreichbarkeit (über Browser)** ▶

**Adresse** ▶

**Kontaktperson** ▶

**Speichern** Zurücksetzen

Abb. 55: Mandanten speichern

**4.4****Mandanten manuell bearbeiten**

- Wählen Sie in der Hauptansicht den Mandanten oder Wiederverkäufer aus, dessen Daten Sie bearbeiten möchten.
- Nehmen Sie in der Detailansicht alle notwendigen Änderungen in den Registerkarten vor. Sie können dabei ohne Zwischenspeicherung zwischen den Registerkarten wechseln, ohne dass Ihre Einstellungen verloren gehen.
- Um nach der Beendigung der Eingaben die Einstellungen zu speichern, klicken Sie auf die Schaltfläche *Speichern*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Zurücksetzen*.

1st-tenant
×

<
Details\*
Extensions
PBX-Agenten-IDs
Chat-IDs
Web Service
>

[? Hilfe](#)

Mandantenname*	1st-tenant
Kunden-ID	
Style	ASC (blue) <span style="float: right;">▼</span>
Standardsprache	Deutsch <span style="float: right;">▼</span>
Personalnummer	200000
Vorname*	1st-Tenant
Nachname*	Admin
E-Mail	
Login*	1st-Tenant-Admin
Passwort*	.....
Passwort bestätigen*	.....
Account sperren	<input type="checkbox"/>
Zeitzone	(UTC+01:00) Europe/Berlin + -

**Systemerreichbarkeit (über Browser)** ▶

**Adresse** ▶

**Kontaktperson** ▶


Speichern

Zurücksetzen

Abb. 56: Änderungen speichern

## 4.5

### Mandanten löschen

- Wählen Sie in der Hauptansicht den Mandanten oder Wiederverkäufer aus, den Sie löschen möchten.  
Ein Wiederverkäufer kann nur gelöscht werden, wenn kein Mandant oder Wiederverkäufer untergeordnet vorhanden ist.
- Klicken Sie in der Symbolleiste auf das Symbol  (Löschen).
- Um den ausgewählten Mandanten wirklich zu löschen, bestätigen Sie die Sicherheitsabfrage.

## 4.6

### OAuth-Login für System aktivieren

neo unterstützt das Login-Verfahren OAuth2 OpenID Connect. Wenn das OAuth-Verfahren für neo konfiguriert wurde, öffnet neo beim Start im Standardbrowser die in der Applikation System Configuration konfigurierte OAuth-Autorisierungs-Webseite, auf der sich der Benutzer anmelden kann. Nach erfolgreicher Authentifizierung wird der Benutzer in der neo-Applikation angemeldet.

- Öffnen Sie in der Navigationsleiste das Mandanten-Modul und wählen Sie in der Hauptansicht den Benutzer *System*.  
⇒ Die Detailansicht öffnet sich.
- Wählen Sie in der Registerkarte *Allgemeine Einstellungen* das Gruppenfeld *Login-Einstellungen*:

System
×

< Details\*
Passwörter
Allgemeine Einstellungen\*
LDAP-Verbindungsdati >

**Inaktivität** ▶

**SMTP-Account** ▶

**SNMP-Agent** ▶

**Login-Einstellungen** ▼

SSO-Login aktivieren

☐

JWT-Login aktivieren

☐

OAuth-Login aktivieren

☒

OAuth-API-Endpunkt

https://authentication.example.org.tol

OAuth-Client-ID

ef0129223a2e3bf76e7c3d8422b15b

Alternative Login-Fehler-Seite

☐ Keine  
☐ Standard  
☒ Benutzerdefiniert

www.Beispiel-Login-Fehler.com

LDAP-Login aktivieren

☐

**Sonstige Einstellungen** ▶

**Nutzungsbedingungen** ▶

Speichern

Zurücksetzen

Abb. 57: OAuth-Login aktivieren (Beispiel)

3. Aktivieren Sie das Kontrollkästchen *OAuth-Login aktivieren* und geben Sie Ihre individuellen OAuth-Einstellungen ein.
4. Klicken Sie auf die Schaltfläche *Speichern*, um die Eingaben zu speichern.  
Klicken Sie auf die Schaltfläche *Abbrechen*, um die Eingaben zu verworfen.

Wenn die Eingaben gespeichert wurden, können Angestellte mit OAuth-Login konfiguriert werden.



Informationen zur Konfiguration finden Sie in der Administrationsanleitung für Mandanten *Benutzerverwaltung Mandant*.

## 5 Angestellten-Modul

Im Angestellten-Modul können Sie Daten zu Benutzern anlegen und verwalten:

- Daten zur Person
- Daten zum Account
- Funktionsrechte für die verschiedenen Applikationen

Sie haben die Möglichkeit einem Benutzer Rollenrechte zuzuweisen, die Sie im Rollen-Modul definieren können. Zusätzlich oder wahlweise können Sie dem Benutzer individuelle Funktionsrechte zuzuweisen.



Einige Funktionsrechte sind an bestimmte Lizenzen gebunden. Diese Funktionsrechte können Sie nur zuweisen, wenn entsprechende (freie) Lizenzen im System vorhanden sind.



Sie können Benutzerdaten auch aus bestehenden [LDAP](#)-Strukturen importieren. Die Konfiguration des Imports erfolgt über das Konfigurationsimport-Modul. Weitere Informationen dazu finden Sie in der Administrationsanleitung *Import von Benutzerdaten*.



Sie können Konfigurationsdaten auch aus bestehenden [LDAP](#)-Strukturen importieren. Die Konfiguration des Imports erfolgt über das Konfigurationsimport-Modul. Weitere Informationen dazu finden Sie in der Administrationsanleitung *Import von Konfigurationsdaten*.

Öffnen Sie das Angestellten-Modul, indem Sie in der Navigationsleiste der Applikation System Configuration auf den Menüpunkt *Angestellte* klicken.

### 5.1 Hauptansicht





In der Hauptansicht werden alle gespeicherten Angestellten angezeigt.

+ × Angestellte Allgemein						
Personalnummer	Vorname	Nachname	E-Mail	Einstellungsdatum	Geburtsdatum	Adresse
111		Agent				
800	8.	Agent				
1100	11.	Agent-Superior				
1000	10.	Agent				
900	9.	Agent				
8000	80.	Agent				
700	7.	Agent				
600	6.	Agent				
500	5.	Agent				
400	4.	Agent				
300	3.	Agent				
200	2.	Agent				

Zeilen pro Seite 50 1 - 14 von 14

Abb. 58: Angestellten-Modul - Hauptansicht

Je nach Konfiguration der Spalten werden die folgenden Informationen in der Hauptansicht angezeigt:






<i>Personalnummer</i>	Personalnummer des Angestellten.
<i>Vorname</i>	Vorname des Angestellten.
<i>Nachname</i>	Nachname des Angestellten.
<i>E-Mail</i>	E-Mail-Adresse des Angestellten.
<i>Einstellungsdatum</i>	Datum, an dem der Angestellte eingestellt wurde.
<i>Geburtsdatum</i>	Geburtsdatum des Angestellten.
<i>Adresse</i>	Private Adresse des Angestellten.
<i>Ist Superuser</i>	Zeigt an, ob der Angestellte Superuser-Rechte hat.  = Superuser-Rechte  = Keine Superuser-Rechte
<i>Sichtbar</i>	Zeigt an, ob der Angestellte für andere Benutzer sichtbar ist.  = Angestellter ist sichtbar  = Angestellter ist nicht sichtbar
<i>Kommentar</i>	Kommentar, der zu den Daten des Angestellten hinzugefügt wurde.
<i>Erstelldatum</i>	Datum, an dem die Daten des Angestellten angelegt wurden.
<i>Aktualisiert</i>	Datum, an dem die Daten des Angestellten zuletzt aktualisiert wurden.

### 5.1.1 Symbolleiste

Die Symbolleiste bietet folgende Funktionen.



Abb. 59: Angestellten-Modul - Symbolleiste

	<i>Suchen</i>	Öffnet das Fenster der Suchfunktion. Mit der Suchfunktion können Sie gezielt nach Datensätzen suchen, die bestimmten Kriterien entsprechen (siehe <a href="#">Kapitel "Suchen", S. 65</a> ). Das Symbol  ( <i>Suchen</i> ) wird immer dann angezeigt, wenn die Suche durch einen Filter angepasst wurde.
	<i>Suche zurücksetzen</i>	Setzt alle manuell gesetzten Suchkriterien zurück. Die Suche wird ohne manuelle Filterung gestartet.
	<i>Erstellen</i>	Legt einen neuen Angestellten an (siehe <a href="#">Kapitel "Neuen Angestellten anlegen", S. 79</a> ).
	<i>Löschen</i>	Löscht den ausgewählten Angestellten (siehe <a href="#">Kapitel "Angestellten löschen", S. 80</a> ).
<i>Angestellte</i>	<i>Zusammenfassung</i>	Listet die Funktionsrechte des ausgewählten Angestellten auf (siehe <a href="#">Kapitel "Zusammenfassung anzeigen", S. 64</a> ).
	<i>Gesperrte Angestellte anzeigen / Alle Angestellten anzeigen</i>	Listet nur die gesperrten Angestellten in der Hauptansicht auf (siehe <a href="#">Kapitel "Gesperrte Angestellte anzeigen", S. 64</a> ).
	<i>Angestellte sichtbar oder nicht sichtbar machen</i>	Funktion, über die der ausgewählte Angestellte für andere sichtbar oder nicht sichtbar geschaltet werden kann (siehe <a href="#">Kapitel "Angestellte sichtbar oder nicht sichtbar machen", S. 65</a> ).
	<i>Benutzerdaten exportieren</i>	Exportiert die Benutzerdaten der Angestellten des aktuellen Mandanten im <a href="#">XML</a> -Format.
<i>Allgemein</i>	<i>Drucken</i>	Druckt die Tabelle der Hauptansicht.

<i>Tabelle anpassen</i>	Öffnet ein Fenster, in dem Sie folgende Einstellungen für die Hauptansicht vornehmen können: <ul style="list-style-type: none"> <li>• Welche Informationen werden angezeigt.</li> <li>• Reihenfolge der angezeigten Spalten.</li> <li>• Anzahl der Zeilen pro Seite</li> </ul>
<i>Allgemeine Hilfe</i>	Über den Menüpunkt <i>Allgemeine Hilfe</i> wird eine Beschreibung der Applikation, in der Sie sich gerade befinden, geöffnet.
<i>Modul-Hilfe</i>	Über den Menüpunkt <i>Modul-Hilfe</i> wird eine Beschreibung des Moduls, in dem Sie sich gerade befinden, geöffnet.



Detaillierte Beschreibungen zu Standardfunktionen wie z. B. *Drucken*, *Tabelle anpassen* oder *Hilfe* finden Sie in der Bedienungsanleitung für Administratoren *Allgemeine Informationen zur System Configuration*.

#### 5.1.1.1 Zusammenfassung anzeigen

Mit dieser Funktion können Sie die Funktionsrechte des Angestellten anzeigen lassen.

1. Wählen Sie den entsprechenden Angestellten aus der Liste in der Hauptansicht aus.
2. Klicken Sie in der Symbolleiste im Menü *Angestellte* auf den Menüpunkt *Zusammenfassung*.
  - ⇒ Das Fenster *Zusammenfassung* erscheint.

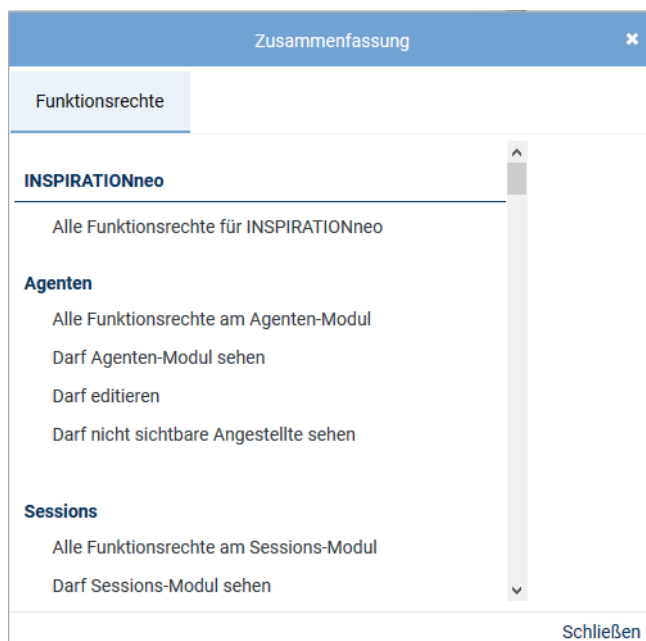




Abb. 60: Zusammenfassung der Funktionsrechte

	Funktionsrecht ist individuell zugewiesen.
	Funktionsrecht ist über eine Rolle zugewiesen. <b>HINWEIS!</b> Führen Sie die Maus auf das Symbol, um anzuzeigen, durch welche Rolle das Funktionsrecht zugeordnet wurde.

#### 5.1.1.2 Gesperrte Angestellte anzeigen

Mit dieser Funktion können Sie alle Angestellten herausfiltern, deren Account gesperrt wurde.



1. Klicken Sie in der Symbolleiste im Menü *Angestellte* auf den Menüpunkt *Gesperrte Angestellte anzeigen*.  
⇒ In der Hauptansicht werden nur die Angestellten angezeigt, deren Account gesperrt ist.
2. Um den Filter aufzuheben, klicken Sie auf den Menüpunkt *Alle Angestellten anzeigen*.





Informationen dazu, wie man einen Account sperren kann, finden Sie unter [Kapitel "Registerkarte Account", S. 71](#).

#### 5.1.1.3 Angestellte sichtbar oder nicht sichtbar machen

Sie können einen Angestellten für andere Benutzer des Systems sichtbar oder nicht sichtbar machen.

Ist ein Angestellter als nicht sichtbar gekennzeichnet, kann er nur vom Superuser oder von einem Benutzer gesehen werden, der das Funktionsrecht *Darf nicht sichtbare Angestellte sehen* besitzt. Die Einstellung, ob ein Angestellter sichtbar ist oder nicht, wirkt sich auf alle *neo*-Applikationen aus.

Einen Angestellten für andere Benutzer nicht sichtbar zu machen kann z. B. sinnvoll sein, wenn der Angestellte für längere Zeit abwesend ist (z. B. Erziehungsurlaub) und ihm deswegen keine Aufgaben zugewiesen werden sollen.

1. Wählen Sie den entsprechenden Angestellten in der Hauptansicht aus.
2. Klicken Sie in der Symbolleiste im Menü *Angestellte* auf den Menüpunkt *Angestellte sichtbar oder nicht sichtbar machen*.  
⇒ Der Status des Angestellten wird geändert.  
⇒ In der Spalte *Sichtbar* der Hauptansicht wechselt das Symbol:  
 = Angestellter ist sichtbar  
 = Angestellter ist nicht sichtbar

#### 5.1.1.4 Suchen

Mit der Suchfunktion können Sie gezielt nach Datensätzen suchen, die bestimmten Kriterien entsprechen.




1. Klicken Sie in der Symbolleiste auf das Symbol  bzw.  (*Suchen*).  
⇒ Das Fenster *Suchkriterien* erscheint.





Abb. 61: Fenster Suchkriterien (Beispiel)

2. Stellen Sie die entsprechenden Suchkriterien ein.  
**HINWEIS!** Welche Suchkriterien zur Verfügung stehen, ist abhängig vom jeweiligen Modul.
3. Um die Suche zu starten, klicken Sie auf die Schaltfläche *Suchen*.  
Um alle manuell gesetzten Suchkriterien zurückzusetzen, klicken Sie auf die Schaltfläche *Zurücksetzen*.

⇒ Nachdem Sie die Suche durchgeführt haben, werden in der Hauptansicht nur die Datensätze angezeigt, die den eingestellten Suchkriterien entsprechen.

4. Um in der Hauptansicht wieder alle ursprünglichen Datensätze anzuzeigen, also die manuell gesetzten Suchkriterien zurückzusetzen, klicken Sie in der Symbolleiste auf das Symbol  (*Suche zurücksetzen*).

Über die Schaltfläche *Suchen verwalten* haben Sie die Möglichkeit, die definierten Suchkriterien unter einem eindeutigen Namen zu speichern, gespeicherte Suchkriterien zu laden und zu löschen.

Über das Symbol  können Sie ein Suchkriterium als Favorit markieren. Als Favorit markierte Suchkriterien werden im oberen Teil des Fensters *Suchkriterien* zusätzlich angezeigt und durch das Symbol  gekennzeichnet.



Eine detaillierte Beschreibung der Suchfunktion finden Sie in der Bedienungsanleitung *System Configuration - Allgemeine Informationen*.

## 5.2

### Detailansicht

Die Detailansicht enthält Informationen zu Daten und Berechtigungen des ausgewählten Angestellten.

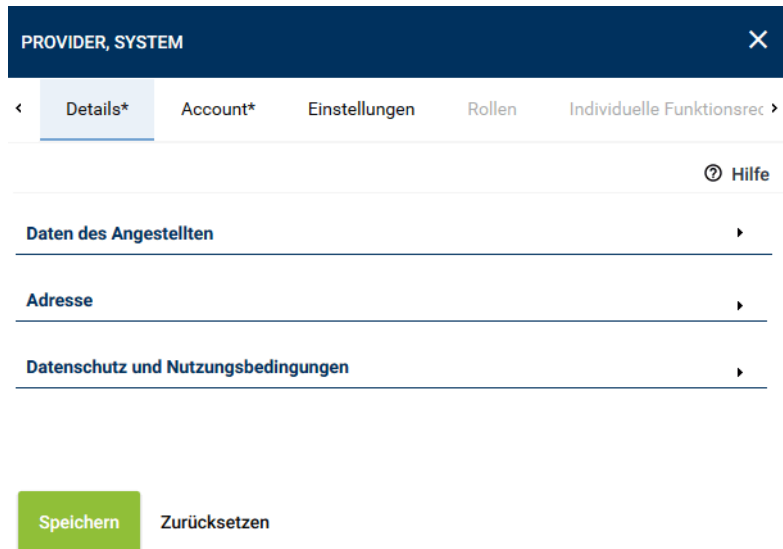


Abb. 62: Angestellten-Modul - Detailansicht

Die Detailansicht besteht aus folgenden Registerkarten:

- *Details*  
Hier können Sie die persönlichen Daten des Angestellten anzeigen und bearbeiten.  
Siehe [Kapitel "Registerkarte Details", S. 67](#).
- *Account*  
Hier können Sie die Login-Daten des Angestellten anzeigen und bearbeiten.  
Siehe [Kapitel "Registerkarte Account", S. 71](#).
- *Einstellungen*  
Hier können Sie Berechtigungen und Protokollierungseinstellungen für den Angestellten anzeigen und bearbeiten.  
Siehe [Kapitel "Registerkarte Einstellungen", S. 74](#).
- *Rollen*  
Hier können Sie die Rollen anzeigen, die dem Angestellten zugewiesen wurden, und die Rollenzuordnung bearbeiten.

Siehe [Kapitel "Registerkarte Rollen", S. 76.](#)

- *Individuelle Funktionsrechte*

Hier können Sie die individuellen Funktionsrechte des Angestellten anzeigen und zuordnen.

Siehe [Kapitel "Registerkarte Individuelle Funktionsrechte", S. 78.](#)

### 5.2.1

#### Registerkarte Details

Hier können Sie die persönlichen Daten des Angestellten anzeigen und bearbeiten.

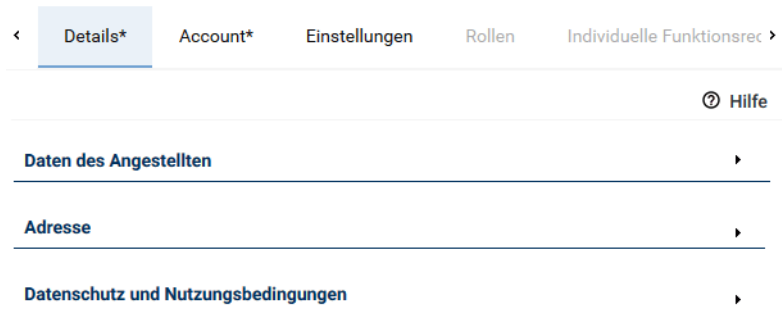



Abb. 63: Angestellten-Modul - Registerkarte Details



Die Angabe einer Adresse ist optional.




Sobald Sie ein Gruppenfeld für optionale Angaben geöffnet haben, müssen Sie die Pflichtfelder in diesem Gruppenfeld ausfüllen, um speichern zu können. Wenn Sie die optionalen Angaben nicht machen möchten, müssen Sie das Gruppenfeld schließen, indem Sie auf das Symbol  der entsprechenden Titelleiste klicken.

#### 5.2.1.1

##### Gruppenfeld Daten des Angestellten

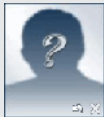
1. Um persönliche Daten des Angestellten zu bearbeiten, öffnen Sie das Gruppenfeld *Daten des Angestellten*.



**Daten des Angestellten**



Personalnummer	100000
Vorname*	SYSTEM
Nachname*	PROVIDER
Geburtsdatum	<input type="text"/>
E-Mail	<input type="text"/>
Einstellungsdatum	<input type="text"/>
Kommentar	<div style="border: 1px solid #ccc; height: 60px;"></div>
Adresse für Wiedergabe per Telefon	<input type="text"/>
Importschlüssel	<input type="text"/>
Zeitzone	UNKNOWN + -

Abb. 64: Daten des Angestellten bearbeiten

	<p>Platzhalter für ein Foto des Angestellten.          Siehe <a href="#">Kapitel "Bild hochladen oder entfernen"</a>, S. 69.</p>
<b>Personalnummer</b>	Personalnummer des Angestellten.
<b>Vorname</b>	Vorname des Angestellten.
<b>Nachname</b>	Nachname des Angestellten.
<b>Geburtsdatum</b>	<p>Geburtsdatum des Angestellten.</p> <p>Die Eingabe des Datums kann direkt über die Tastatur oder über das Symbol erfolgen.</p>
<b>E-Mail</b>	E-Mail-Adresse des Angestellten.
<b>Einstellungsdatum</b>	<p>Tag, an dem der Angestellte eingestellt wurde.</p> <p>Die Eingabe des Datums kann direkt über die Tastatur oder über das Symbol erfolgen.</p>
<b>Kommentar</b>	Kommentar zu den Daten des Angestellten.
<b>Adresse für Wiedergabe per Telefon</b>	<p>Geben Sie hier die Adresse des Telefons an, an dem die Gespräche ausgegeben werden sollen. Je nach dem, welcher Agent sich an diesem Telefon anmeldet, werden die Audiodaten zur Verfügung gestellt, die der Teilnehmer wiedergeben darf. Sie können folgende Zusatzdaten als Adresse verwenden:</p> <ul style="list-style-type: none"> <li>• Extension, wenn diese in der PBX für die Wiedergabe per Telefon konfiguriert ist.</li> <li>• Komplette Telefonnummer, z. B. 06021 5001 1015, wenn die PBX am öffentlichen Telefonnetz hängt.</li> <li>• IP-Adresse, wenn diese konfiguriert ist.</li> </ul>

	<ul style="list-style-type: none"> <li>• MAC-Adresse, wenn diese konfiguriert ist.</li> <li>• SIP-Adresse, z. B. <i>Extension@IP-Adresse</i>.</li> </ul>
<b>Importschlüssel</b>	<p>Schlüssel zur eindeutigen Identifizierung eines aus einer externen Quelle importierten Angestellten.</p> <p>Beim ersten Import der Daten des Angestellten wird der Importschlüssel automatisch hier eingetragen. Bei jedem erneuten Import wird anhand dieses Importschlüssels abgeglichen, ob der Angestellte bereits zuvor importiert wurde.</p> <p>Der Importsschlüssel wird außerdem bei der Übertragung (Export/Import) von Aufzeichnungen aus einem <i>neo</i>-System in ein anderes <i>neo</i>-System verwendet, um die Aufzeichnungen den Agenten zuzuordnen. Falls der Angestellte keinen automatisch angelegten Importschlüssel hat, können Sie für diese Zuordnung manuell einen Importschlüssel eintragen.</p> <p><b>HINWEIS!</b> Wenn Sie einen Importschlüssel manuell ändern, wird der Angestellte bei einem erneuten Import von Angestellten Daten nicht als bereits importierter Angestellter erkannt. Außerdem können bei einem erneuten Import von Aufzeichnungen die Aufzeichnungen nicht korrekt zugeordnet werden.</p>
<b>Zeitzone</b>	<p>Zeigt die Zeitzone, in der die Konversationen in den Wiedergabeapplikationen angezeigt werden sollen. Die Einstellungen, die Sie für den jeweiligen Angestellten konfigurieren, sind der Voreinstellung im Mandanten-Modul übergeordnet.</p> <p>Um die Zeitzone auszuwählen, klicken Sie auf die Schaltfläche . Siehe <a href="#">Kapitel "Zeitzone hinzufügen", S. 18</a>.</p> <p>Um die Auswahl zu löschen, klicken Sie auf die Schaltfläche .</p>

#### 5.2.1.1.1 Bild hochladen oder entfernen

1. Klicken Sie auf das Symbol  (*Bild hochladen*) auf dem Platzhalter für das Foto.

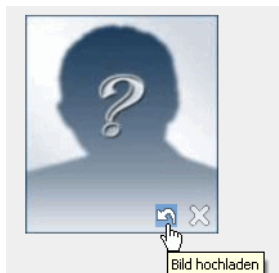


Abb. 65: Bild hochladen

⇒ Das Fenster *Datei hochladen* erscheint.



Abb. 66: Datei hochladen

2. Klicken Sie auf die Schaltfläche *Datei auswählen*.
3. Wählen Sie über den Explorer die Datei aus und klicken Sie auf die Schaltfläche *Öffnen*.

Sie können mehrere Bilddateien in diese Zwischenablage legen.




Um die Zwischenablage zu leeren, klicken Sie auf die Schaltfläche *Alle Dateien entfernen*.

Um nur eine Bilddatei aus der Zwischenablage zu entfernen, klicken Sie auf die Schaltfläche



neben der Datei.

4. Um ein Bild in die Detailansicht zu übernehmen, klicken Sie auf die Schaltfläche *Datei hochladen*.  
⇒ Das Bild wird in der Detailansicht angezeigt.
5. Falls Sie ein Bild wieder entfernen möchten, klicken Sie auf das Symbol  (*Bild entfernen*) in der rechten unteren Ecke des Bildes.

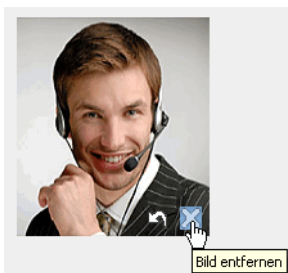


Abb. 67: Bild entfernen (Beispiel)


⇒ Das Bild wird aus der Detailansicht gelöscht.

### 5.2.1.2 Gruppenfeld Adresse

1. Falls Sie eine Kontaktadresse hinzufügen möchten, öffnen Sie das Gruppenfeld *Adresse*.



Abb. 68: Adresse hinzufügen

2. Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Adresse hinzufügen*.
3. Geben Sie die Adresse ein.

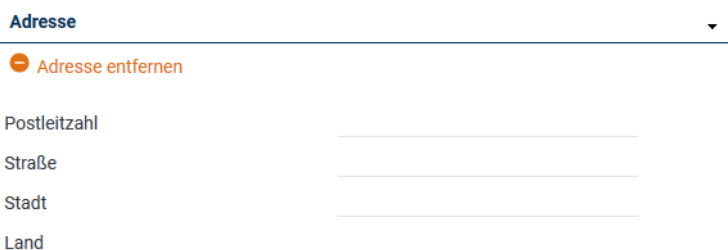



Abb. 69: Adresse hinzufügen

4. Falls Sie die Adresse entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Adresse entfernen*.

### 5.2.1.3 Gruppenfeld Datenschutz und Nutzungsbedingungen

1. Falls Sie Datenschutz und Nutzungsbedingungen hinzufügen möchten, öffnen Sie das Gruppenfeld *Datenschutz und Nutzungsbedingungen*.

### Datenschutz und Nutzungsbedingungen

[+ Link hinzufügen](#)

Abb. 70: Datenschutz und Nutzungsbedingungen hinzufügen

- Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche [+ Link hinzufügen](#).
- Geben Sie die entsprechenden Links ein.

### Datenschutz und Nutzungsbedingungen

[- Entfernen](#)

Offizielle Datenschutzerklärung

Datenschutzerklärung (Ersatz)

Offizielles Impressum

Impressum (Ersatz)

Abb. 71: Datenschutz und Nutzungsbedingungen hinzufügen

<b>Offizielle Datenschutzerklärung</b>	Geben Sie hier den Link für die Offizielle Datenschutzerklärung ein.
<b>Datenschutzerklärung (Ersatz)</b>	Geben Sie hier den Link für die Datenschutzerklärung (Ersatz) ein.
<b>Offizielles Impressum</b>	Geben Sie hier den Link für das Offizielle Impressum ein.
<b>Impressum (Ersatz)</b>	Geben Sie hier den Link für das Impressum (Ersatz) ein.

- Falls Sie die Datenschutz und Nutzungsbedingungen entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche [- Entfernen](#).

## 5.2.2

### Registerkarte Account

Hier können Sie die Login-Daten des Angestellten anzeigen und bearbeiten. Erst wenn Sie einen Account für den Angestellten angelegt haben, werden die übrigen Registerkarten freigeschaltet.

Details\*
Account\*
Einstellungen
Rollen
Individuelle Funktionsrec

Account

Account entfernen

Benutzername\*
9Agent

Passwort\*

Passwort bestätigen\*

Passwort beim nächsten Login ändern
☐

Läuft niemals ab
☐

Passwortregeln müssen nicht erfüllt werden.
☐

Account sperren
☐

LDAP

Kombinations-Login

Details\*
Account\*
Einstellungen
Rollen
Individuelle Funktionsrec

Account

Account entfernen

Benutzername\*
System-Admin

Passwort\*

Passwort bestätigen\*

Passwort beim nächsten Login ändern
☐

Account sperren
☐

LDAP

Kombinations-Login

Abb. 72: Angestellten-Modul - Registerkarte Account




Für Angestellte mit Superuser-Rechten werden einige Optionen ausgeblendet.



Die Eingabe von Account-Daten ist optional.




Sobald Sie ein Gruppenfeld für optionale Angaben geöffnet haben, müssen Sie die Pflichtfelder in diesem Gruppenfeld ausfüllen, um speichern zu können. Wenn Sie die optionalen Angaben nicht machen möchten, müssen Sie das Gruppenfeld schließen, indem Sie auf das Symbol  der entsprechenden Titelleiste klicken.


1. Um einen Account neu anzulegen, öffnen Sie das Gruppenfeld *Account*.



Abb. 73: Account hinzufügen

2. Klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Account hinzufügen*.
3. Geben Sie alle erforderlichen Daten ein.

<i>Benutzername</i>	<p>Geben Sie hier den Benutzernamen ein, mit dem sich der Angestellte am System anmelden muss.</p> <p><b>HINWEIS!</b> Falls Sie die Funktion <i>Last Call Repeat</i> benutzen, dürfen Sie hier ausschließlich Zahlen verwenden.</p> <p><b>HINWEIS!</b> Falls Sie die Funktion SSO-Login nutzen, muss der Benutzername aus dem Windows-Benutzernamen und der Domain bestehen. Format: <i>Domain\Windows-Benutzername</i></p>
<i>Passwort</i>	<p>Geben Sie hier das Passwort ein, mit dem sich der Angestellte am System anmelden muss.</p> <p><b>HINWEIS!</b> Falls Sie die Funktion <i>Last Call Repeat</i> benutzen, dürfen Sie hier ausschließlich Zahlen verwenden.</p>
<i>Passwort bestätigen</i>	Geben Sie hier erneut das Passwort für den Angestellten ein.
<i>Passwort beim nächsten Login ändern</i>	Aktivieren Sie diese Option, wenn der Angestellte sein Passwort beim nächsten Login ändern soll.
<i>Läuft niemals ab</i>	<p>Aktivieren Sie diese Option, wenn das Passwort niemals ungültig werden soll.</p> <p><b>HINWEIS!</b> Diese Option steht für Superuser nicht zur Verfügung.</p>
<i>Passwortregeln müssen nicht erfüllt werden</i>	<p>Aktivieren Sie diese Option, wenn das Passwort nicht den definierten Passwortregeln entsprechen muss.</p> <p><b>HINWEIS!</b> Passwortregeln können Sie im Mandanten-Modul in der Registerkarte <i>Passwörter</i> definieren.</p> <p><b>HINWEIS!</b> Diese Option steht für Superuser nicht zur Verfügung.</p>
<i>Account sperren</i>	<p>Mit dieser Option können Sie den Account des Angestellten sperren. In der Hauptansicht können Sie nach diesem Kriterium filtern, siehe <a href="#">Kapitel "Gesperrte Angestellte anzeigen", S. 64</a>.</p> <p><b>HINWEIS!</b> Diese Option steht für Superuser nicht zur Verfügung.</p>

4. Falls Sie den Account entfernen möchten, klicken Sie in der Titelleiste des Gruppenfelds auf die Schaltfläche  *Account entfernen*.
5. Um die Authentifizierung via [LDAP](#) für den Angestellten zu aktivieren, siehe [Kapitel "Authentifizierung via LDAP", S. 72](#).
6. Um dem Angestellten einen Kombinationsbenutzer zuzuordnen, siehe [Kapitel "Kombinationsbenutzer zuordnen", S. 73](#).

#### 5.2.2.1 Authentifizierung via LDAP

1. Um die Authentifizierung via [LDAP](#) zu aktivieren, öffnen Sie das Gruppenfeld *LDAP*.



2. Aktivieren Sie das Kontrollkästchen *LDAP-Authentifizierung*.



Abb. 74: Authentifizierung via LDAP aktivieren

3. Geben Sie im Feld *LDAP-DN* den kompletten Distinguished Name (DN) des Benutzers ein.
4. Falls Sie die Authentifizierung via LDAP wieder deaktivieren möchten, deaktivieren Sie das Kontrollkästchen *LDAP-Authentifizierung*.

- ☒ = Authentifizierung via **LDAP** ist aktiviert  
☐ = Authentifizierung via **LDAP** ist nicht aktiviert


### 5.2.2.2 Kombinationsbenutzer zuordnen

Aus Sicherheitsgründen kann es in ein oder anderen Fall sinnvoll sein, Kombinationsbenutzer zuzuordnen.



Wenn Sie einem Benutzer 1 Kombinationsbenutzer zuordnen, kann sich dieser Benutzer nur gemeinsam mit dem Kombinationsbenutzer am System anmelden.

Wenn Sie einem Benutzer mehrere Kombinationsbenutzer zuordnen, kann sich dieser Benutzer nur gemeinsam mit mindestens 1 der Kombinationsbenutzer am System anmelden.

1. Öffnen Sie das Gruppenfeld *Kombinations-Login*.
2. Klicken Sie auf das Symbol  (*Hinzufügen*).

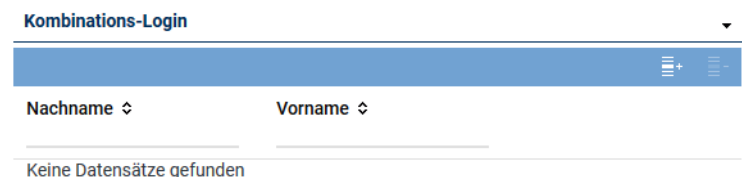
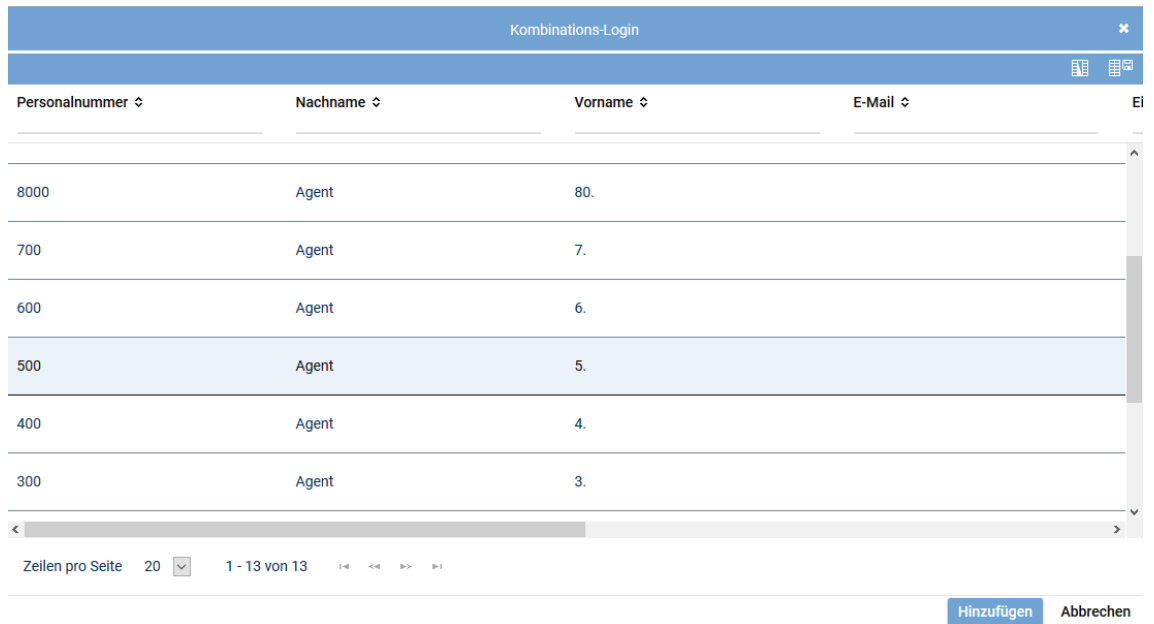


Abb. 75: Kombinationsbenutzer zuordnen

3. Wählen Sie einen oder mehrere Kombinationsbenutzer aus der Liste aus.  
 Um mehrere Kombinationsbenutzer auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.



Personalnummer	Nachname	Vorname	E-Mail
8000	Agent	80.	
700	Agent	7.	
600	Agent	6.	
500	Agent	5.	
400	Agent	4.	
300	Agent	3.	


Zeilen pro Seite: 20 1 - 13 von 13

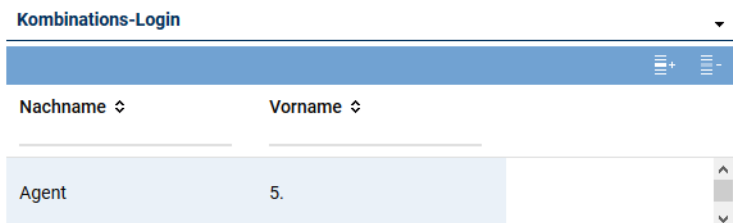
Hinzufügen Abbrechen

Abb. 76: Kombinationsbenutzer hinzufügen

- Um die ausgewählten Kombinationsbenutzer hinzuzufügen, klicken Sie auf die Schaltfläche *Hinzufügen*.  
Um die Auswahl zu verwerfen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

### 5.2.2.3 Kombinationsbenutzer-Zuordnung löschen

- Öffnen Sie das Gruppenfeld *Kombinations-Login*.
- Um die Zuordnung eines Kombinationsbenutzers zu löschen, wählen Sie den entsprechenden Kombinationsbenutzer in der Liste aus und klicken Sie auf das Symbol  (*Entfernen*).



Nachname	Vorname
Agent	5.

Hinzufügen Abbrechen

Abb. 77: Kombinationsbenutzer-Zuordnung löschen

### 5.2.3 Registerkarte Einstellungen

Hier können Sie die Berechtigungen und Protokollierungseinstellungen des Benutzers anzeigen und bearbeiten.

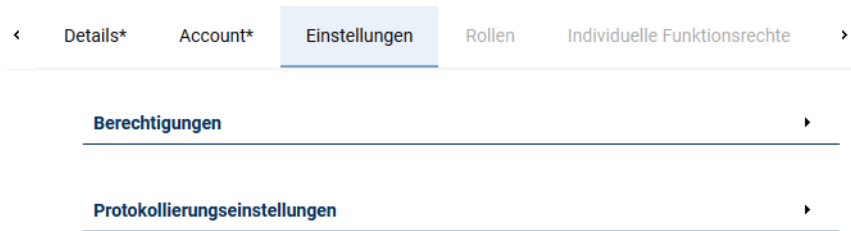


Abb. 78: Angestellten-Modul - Registerkarte Einstellungen

### 5.2.3.1 Gruppenfeld Berechtigungen

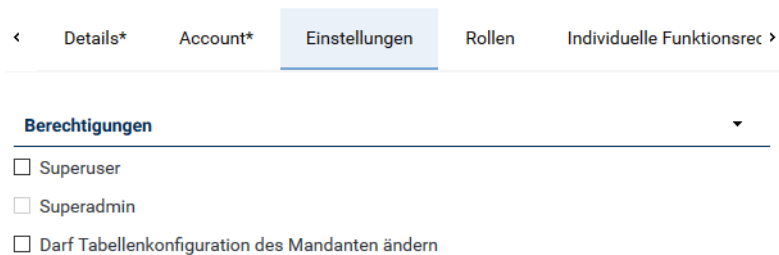


Abb. 79: Berechtigungen einstellen

<b>Superuser</b>	<p>Mit diesem Recht erhält der Benutzer alle Funktionsrechte im System, zu denen auch Lizenzen zur Verfügung stehen.</p> <p><input checked="" type="checkbox"/> = Recht ist aktiviert  <input type="checkbox"/> = Recht ist deaktiviert</p>
<b>Superadmin</b>	<p>Mit diesem Recht erhält der Benutzer eingeschränkte Superuser-Funktionsrechte im System.</p> <p>Angestellte des Systembetreibers, die als Superadmin konfiguriert sind, können sich bei jedem im System vorhandenen Mandanten mit den Befugnissen eines Superusers dieses Mandanten in folgenden Applikationen anmelden.</p> <ul style="list-style-type: none"> <li>• System Configuration</li> <li>• System Monitoring</li> <li>• Portal</li> </ul> <p>Informationen zum Superadmin-Login finden Sie entsprechend der Applikation in den Bedienungsanleitungen <i>System Configuration - Allgemeine Informationen</i>, <i>System Monitoring</i> und <i>Portal</i>.</p> <p>Ein Superadmin hat keinen Zugriff auf Aufzeichnungen.</p> <p>Ein Superadmin kann keiner Organisationseinheit zugeordnet werden.</p> <p><input checked="" type="checkbox"/> = Recht ist aktiviert  <input type="checkbox"/> = Recht ist deaktiviert</p> <p><b>HINWEIS!</b>  Superadmin-Rechte sind nur in einer Cloud-Umgebung verfügbar und müssen bei Bedarf freigeschaltet werden.  Die Option <i>Superadmin</i> wird nur angezeigt, wenn die entsprechende Lizenz im System vorhanden ist.  In einem Single-Mandanten-System wird die Option <i>Superadmin</i> automatisch aktiviert. Hier ist keine Extra-Lizenz erforderlich.  Für den vom System angelegten Standard-Superuser steht die Option <i>Superadmin</i> nicht zur Verfügung.</p>

*Darf Tabellenkonfiguration des Mandanten ändern*

Mit diesem Recht kann der Benutzer die Standard-Tabellenkonfiguration für die Angestellten des Mandanten ändern.

Dies gilt für die Hauptansicht der jeweiligen Module, sowie für Dialogfenster.



Sobald Sie einem Benutzer Superuser-Rechte zuweisen, sind nur noch die Registerkarten *Details*, *Account* und *Einstellungen* aktiv. In allen anderen Registerkarten sind in diesem Fall keine weiteren Einstellungen nötig.

### 5.2.3.2

#### Gruppenfeld Protokollierungseinstellungen

##### Protokollierungseinstellungen

Protokollierung folgender Aktivitäten des Anwenders

☐ Zugangskontrolle

☐ Konfigurationsaktivitäten

Abb. 80: Protokollierung einstellen

Mit den Optionen in diesem Gruppenfeld haben Sie die Möglichkeit, ausgewählte Aktivitäten des Benutzers zu protokollieren.

☒ = Protokollierung ist aktiviert

☐ = Protokollierung ist deaktiviert

*Zugangskontrolle*

Ist diese Option aktiviert, wird protokolliert, wann sich der Benutzer am System an- und abgemeldet hat.

*Konfigurationsaktivitäten*

Ist diese Option aktiviert, werden die Aktivitäten protokolliert, mit denen der Benutzer Konfigurationen angepasst hat.

### 5.2.4

#### Registerkarte Rollen

Hier können Sie dem Angestellten (Benutzer) definierte Rollen zuordnen.



Rollen können Sie im Rollen-Modul definieren.



Abb. 81: Angestellten-Modul - Registerkarte Rollen


Durch die Zuordnung einer Rolle wird der Benutzer Mitglied dieser Rolle und besitzt dadurch alle Rechte, die für diese Rolle vergeben wurden.



Im Angestellten-Modul können Sie den Umfang der Funktionsrechte, die einem Benutzer über eine Rolle zugewiesen wurden, mit individuellen Funktionsrechten ergänzen.

#### 5.2.4.1

#### Rollen zuordnen

1. Klicken Sie auf das Symbol  (*Hinzufügen*).

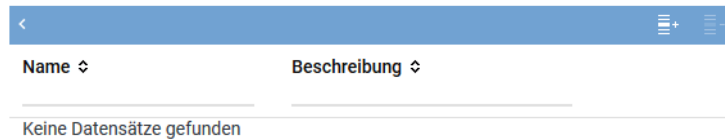


Abb. 82: Rollen zuordnen

2. Wählen Sie eine oder mehrere Rollen aus der Liste aus.  
Um mehrere Rollen auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.

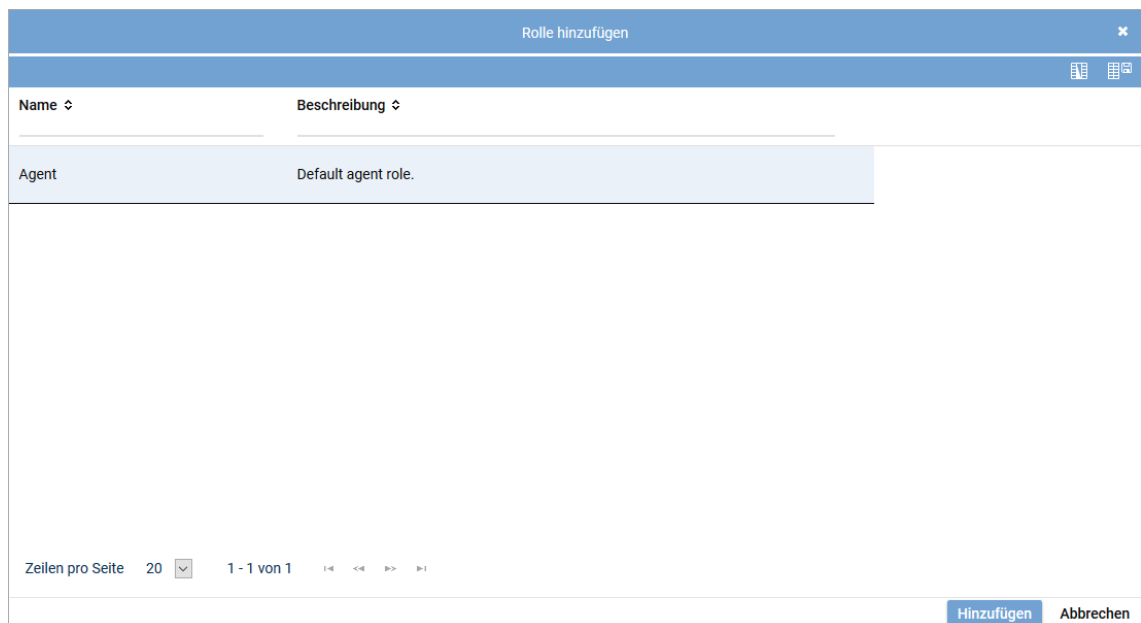



Abb. 83: Rolle hinzufügen

3. Um die ausgewählten Rollen hinzuzufügen, klicken Sie auf die Schaltfläche *Hinzufügen*.  
Um die Auswahl zu verwerfen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

#### 5.2.4.2

#### Rollenzuordnung löschen

1. Wählen Sie die Rolle, die Sie entfernen möchten, in der Liste aus und klicken Sie auf das Symbol  (*Entfernen*).

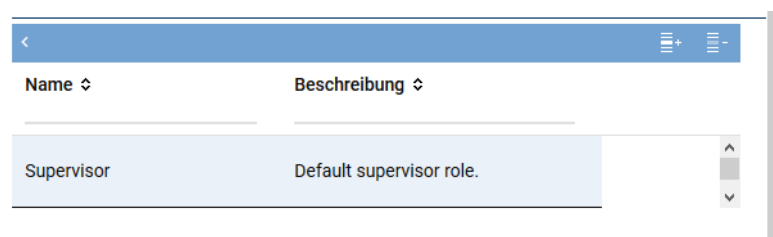


Abb. 84: Rollenzuordnung löschen



Eine Änderung der Rollenzuordnung wird erst wirksam, wenn sich der Benutzer das nächste Mal am System anmeldet.

### 5.2.5 Registerkarte Individuelle Funktionsrechte

Hier können Sie die individuellen Funktionsrechte des Angestellten anzeigen und zuordnen.

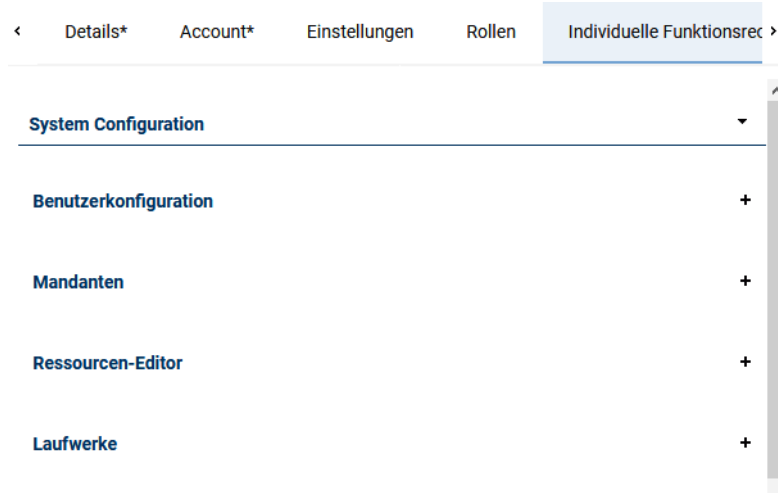


Abb. 85: Angestellten-Modul - Registerkarte Individuelle Funktionsrechte (Beispiel)

Sie können die Funktionsrechte für die verschiedenen *neo*-Applikationen individuell vergeben.

- Um die Funktionsrechte an einer Applikation anzupassen, öffnen Sie das Gruppenfeld mit dem entsprechenden Applikationsnamen.  
⇒ Alle Teilbereiche der Applikation werden aufgelistet.

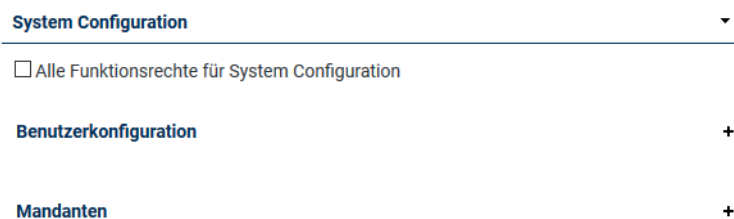


Abb. 86: Funktionsrechte - Teilbereiche anzeigen (Beispiel)

- Falls Sie dem Benutzer pauschal alle Funktionsrechte an einer Applikation zuweisen möchten, aktivieren Sie das Kontrollkästchen *Alle Funktionsrechte für ....* Dieses Recht ist übergeordnet und gilt für alle Module dieser Applikation.



Die Option, alle Funktionsrechte zu einer Applikation pauschal zuzuweisen, steht nicht für alle Applikationen zur Verfügung.


- Falls Sie die Funktionsrechte selektiv zuweisen möchten, öffnen Sie die Details zu einem Teilbereich (z. B. einem Modul), indem Sie auf das Symbol "+" in der Zeile mit dem entsprechenden Text klicken.  
⇒ Alle Funktionsrechte zu diesem Teilbereich werden eingeblendet.

**System Configuration** ▾

---




☐ Alle Funktionsrechte für System Configuration

**Benutzerkonfiguration** -

Name	Typ	Rolle
<input type="checkbox"/> Darf Benutzer konfigurieren		

**Mandanten** +

Abb. 87: Funktionsrechte - Funktionsrechte anzeigen


(1. Spalte)	Zeigt an, ob das Funktionsrecht individuell zugewiesen wurde. <input checked="" type="checkbox"/> = individuelles Funktionsrecht <input type="checkbox"/> = kein individuelles Funktionsrecht
Name	Beschreibung des Funktionsrechts.
Typ	Zeigt an, welche Lizenz für dieses Recht benötigt wird.  = Agenten-Lizenz  = Supervisoren-Lizenz  = Basis-Lizenz (ohne Agenten- oder Supervisoren-Rechte)
Rolle	Zeigt an, ob das Funktionsrecht dem Benutzer über eine Rolle zugewiesen wurde (Rollenrecht). keine Markierung = kein Rollenrecht <input checked="" type="checkbox"/> = Rollenrecht <b>HINWEIS!</b> Über welche Rolle ein Funktionsrecht zugewiesen wurde, können Sie im Fenster <i>Zusammenfassung</i> sehen, siehe <a href="#">Kapitel "Zusammenfassung anzeigen"</a> , S. 64.

Tab. 3: Funktionsrechte

- Um alle Funktionsrechte für einen Teilbereich zuzuweisen, aktivieren Sie das entsprechende Kontrollkästchen *Alle Funktionsrechte am...*  
Um nur einzelne Funktionsrechte zuzuweisen, aktivieren Sie nur die Kontrollkästchen zu den Funktionsrechten, die Sie zuweisen möchten.
- Falls Sie die Details zu einem Teilbereich wieder ausblenden möchten, klicken Sie auf das Symbol "-" in der Zeile mit dem entsprechendem Text.

### 5.3

#### Neuen Angestellten anlegen

- Klicken Sie in der Symbolleiste auf das Symbol  (*Erstellen*).
- Nehmen Sie in den Registerkarten der Detailansicht alle Einstellungen vor, wie in den entsprechenden Kapiteln beschrieben.  
Sie können dabei ohne Zwischenspeicherung zwischen den Registerkarten wechseln, ohne dass Ihre Einstellungen verloren gehen.
- Um nach der Beendigung der Eingaben die Einstellungen zu speichern, klicken Sie auf die Schaltfläche *Speichern*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Zurücksetzen*.

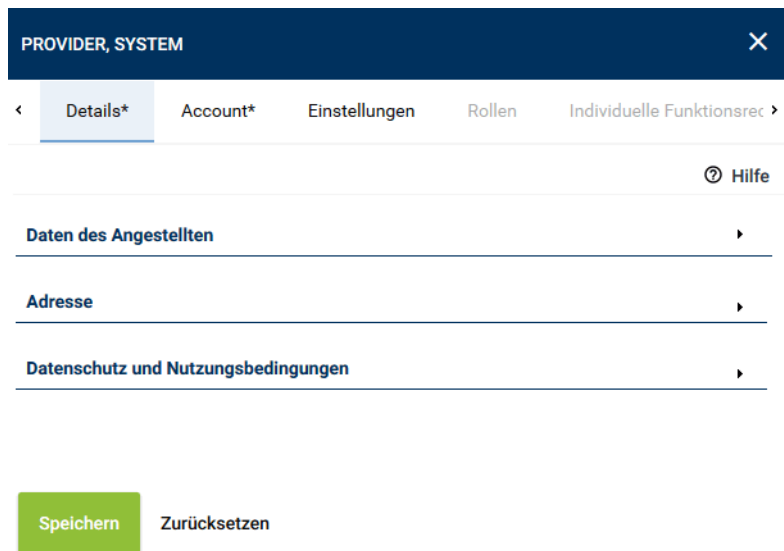


Abb. 88: Angestellten speichern

## 5.4

**Angestellten bearbeiten**

1. Wählen Sie in der Hauptansicht den Angestellten aus, dessen Daten Sie bearbeiten möchten.
2. Nehmen Sie in den Registerkarten der Detailansicht alle notwendigen Änderungen vor. Sie können dabei ohne Zwischenspeicherung zwischen den Registerkarten wechseln, ohne dass Ihre Einstellungen verloren gehen.
3. Um nach der Beendigung der Eingaben die Einstellungen zu speichern, klicken Sie auf die Schaltfläche *Speichern*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Zurücksetzen*.

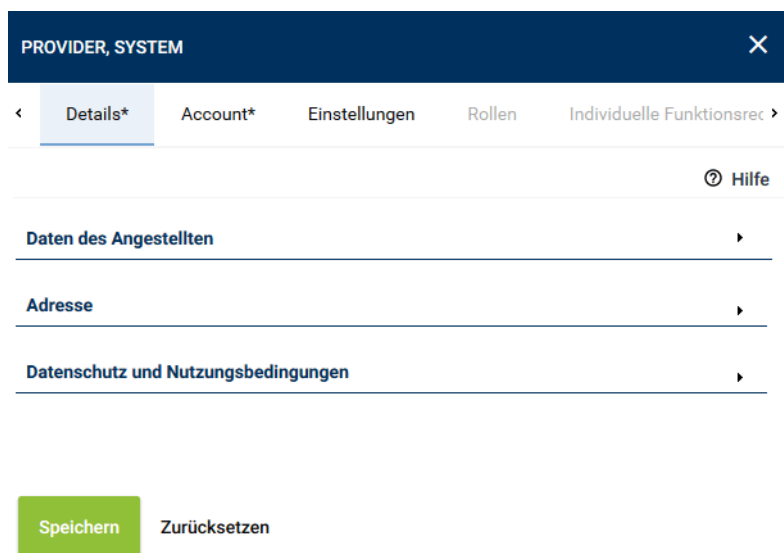



Abb. 89: Änderungen speichern

## 5.5

**Angestellten löschen**

1. Wählen Sie in der Hauptansicht den Angestellten aus, den Sie löschen möchten.
2. Klicken Sie in der Symbolleiste auf das Symbol  (*Löschen*).
3. Um den ausgewählten Angestellten wirklich zu löschen, bestätigen Sie die Sicherheitsabfrage.





---

Falls der gelöschte Angestellte als Kombinationsbenutzer zugeordnet war, erhalten Sie eine entsprechende Warnung.

---



---

Wenn Sie einen Angestellten löschen während dieser als Benutzer am System angemeldet ist, wird die Löschung des Profils erst wirksam, nachdem er sich vom System abgemeldet hat.

---

## 6 Rollen-Modul

Im Rollen-Modul können Sie verschiedene Rollen anlegen und diesen Rollen ausgewählte Funktionsrechte an den verschiedenen Applikationen zuzuordnen.

Indem Sie einem Benutzer eine Rolle zuordnen, weisen Sie ihm automatisch alle Funktionsrechte dieser Rolle zu. Wenn Sie einem Benutzer mehrere Rollen zuordnen, erhält er alle Funktionsrechte, die in Summe in diesen Rollen enthalten sind.



Im Angestellten-Modul können Sie den Umfang der Funktionsrechte, die einem Benutzer über eine Rolle zugewiesen wurden, mit individuellen Funktionsrechten ergänzen.



Sie können Benutzerdaten auch aus bestehenden [LDAP](#)-Strukturen importieren. Die Konfiguration des Imports erfolgt über das Konfigurationsimport-Modul. Weitere Informationen dazu finden Sie in der Administrationsanleitung *Import von Benutzerdaten*.

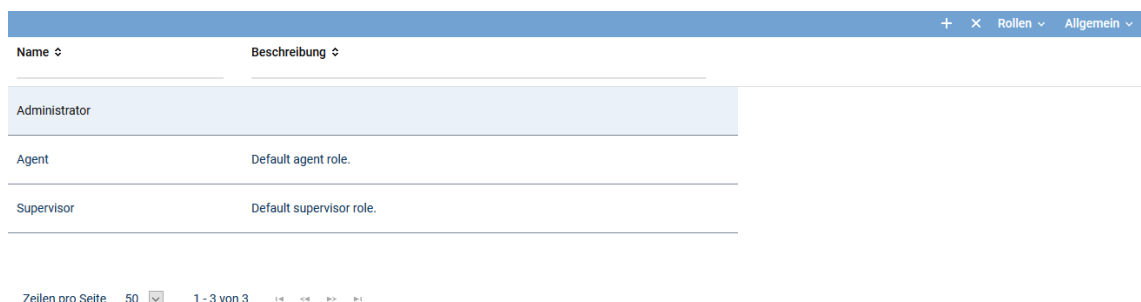


Sie können Konfigurationsdaten auch aus bestehenden [LDAP](#)-Strukturen importieren. Die Konfiguration des Imports erfolgt über das Konfigurationsimport-Modul. Weitere Informationen dazu finden Sie in der Administrationsanleitung *Import von Konfigurationsdaten*.

Öffnen Sie das Rollen-Modul, indem Sie in der Navigationsleiste der Applikation System Configuration auf den Menüpunkt *Rollen* klicken.

### 6.1 Hauptansicht

In der Hauptansicht werden alle gespeicherten Rollen angezeigt.



Name	Beschreibung
Administrator	
Agent	Default agent role.
Supervisor	Default supervisor role.

Abb. 90: Rollen-Modul - Hauptansicht

Je nach Konfiguration der Spalten werden die folgenden Informationen in der Hauptansicht angezeigt:


<i>Name</i>	Name der Rolle.
<i>Beschreibung</i>	Beschreibung der Rolle.
<i>Erstelldatum</i>	Datum, an dem die Rolle erstellt wurde.
<i>Aktualisiert</i>	Datum, an dem die Rolle zuletzt aktualisiert wurde.






#### 6.1.1 Symbolleiste

Die Symbolleiste bietet folgende Funktionen.



Abb. 91: Rollen-Modul - Symbolleiste

	<i>Suchen</i>	Öffnet das Fenster der Suchfunktion. Mit der Suchfunktion können Sie gezielt nach Datensätzen suchen, die bestimmten Kriterien entsprechen (siehe <a href="#">Kapitel "Suchen", S. 65</a> ).
---	---------------	--

		Das Symbol  ( <i>Suchen</i> ) wird immer dann angezeigt, wenn die Suche durch einen Filter angepasst wurde.
	<i>Suche zurücksetzen</i>	Setzt alle manuell gesetzten Suchkriterien zurück. Die Suche wird ohne manuelle Filterung gestartet.
	<i>Erstellen</i>	Legt eine neue Rolle an (siehe <a href="#">Kapitel "Neue Rolle anlegen"</a> , S. 87).
	<i>Löschen</i>	Löscht die ausgewählte Rolle (siehe <a href="#">Kapitel "Rolle löschen"</a> , S. 89).
<i>Rollen</i>	<i>Duplizieren mit Angestellten</i>	Legt eine Kopie der ausgewählten Rolle mit den zugeordneten Angestellten an (siehe <a href="#">Kapitel "Rolle duplizieren"</a> , S. 87).
	<i>Duplizieren ohne Angestellte</i>	Legt eine Kopie der ausgewählten Rolle ohne die zugeordneten Angestellten an (siehe <a href="#">Kapitel "Rolle duplizieren"</a> , S. 87).
<i>Allgemein</i>	<i>Drucken</i>	Druckt die Tabelle der Hauptansicht.
	<i>Tabelle anpassen</i>	Öffnet ein Fenster, in dem Sie folgende Einstellungen für die Hauptansicht vornehmen können: <ul style="list-style-type: none"> <li>• Welche Informationen werden angezeigt.</li> <li>• Reihenfolge der angezeigten Spalten.</li> <li>• Anzahl der Zeilen pro Seite</li> </ul>
	<i>Allgemeine Hilfe</i>	Über den Menüpunkt <i>Allgemeine Hilfe</i> wird eine Beschreibung der Applikation, in der Sie sich gerade befinden, geöffnet.
	<i>Modul-Hilfe</i>	Über den Menüpunkt <i>Modul-Hilfe</i> wird eine Beschreibung des Moduls, in dem Sie sich gerade befinden, geöffnet.



Detaillierte Beschreibungen zu Standardfunktionen wie z. B. *Drucken*, *Tabelle anpassen* oder *Hilfe* finden Sie in der Bedienungsanleitung für Administratoren *Allgemeine Informationen zur System Configuration*.

## 6.2

### Detailansicht

Die Detailansicht enthält Daten und Informationen zur ausgewählten Rolle.

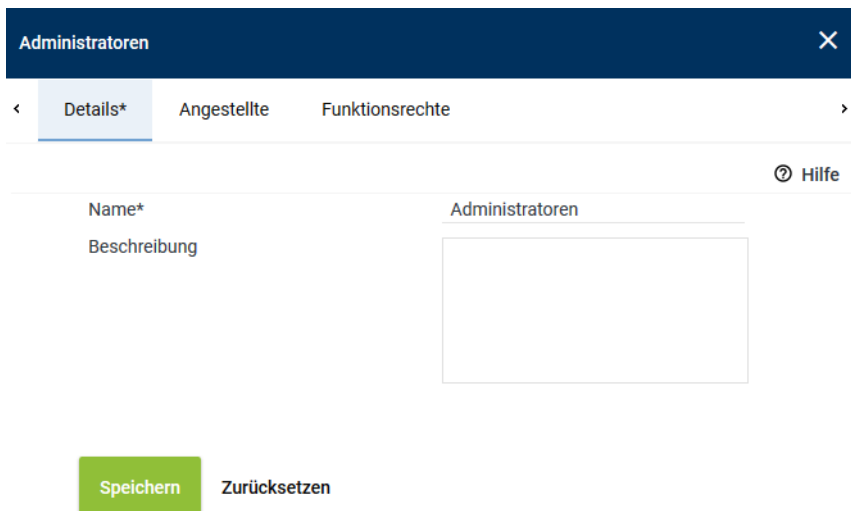


Abb. 92: Rollen-Modul - Detailansicht

Die Detailansicht besteht aus folgenden Registerkarten:

- *Details*

Hier können Sie den Namen und die Beschreibung der Rolle anzeigen und bearbeiten.

Siehe [Kapitel "Registerkarte Details", S. 84.](#)

- *Angestellte*

Hier können Sie die Benutzer anzeigen, denen die Rolle zugewiesen wurde und die Benutzerzuordnung bearbeiten.

Siehe [Kapitel "Registerkarte Angestellte", S. 84.](#)

- *Funktionsrechte*

Hier können Sie die Funktionsrechte der Rolle anzeigen und zuweisen.

Siehe [Kapitel "Registerkarte Funktionsrechte", S. 85.](#)

### 6.2.1 Registerkarte Details

Hier können Sie den Namen und die Beschreibung der Rolle anzeigen und bearbeiten.

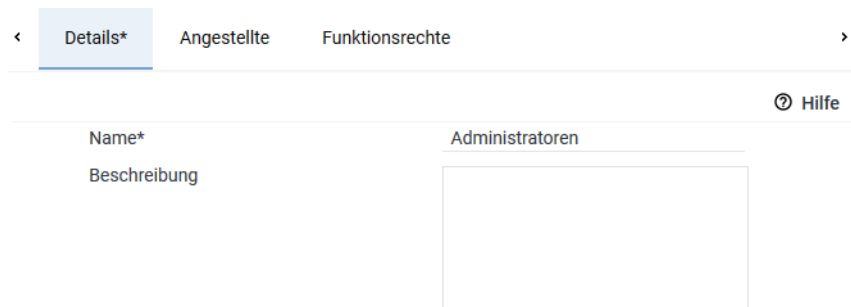


Abb. 93: Rollen-Modul - Registerkarte Details

<i>Name</i>	Name der Rolle.
<i>Beschreibung</i>	Beschreibung der Rolle.

### 6.2.2 Registerkarte Angestellte

Hier können Sie der Rolle ausgewählte Angestellte (Benutzer) zuordnen.

Durch die Zuordnung einer Rolle wird der Benutzer Mitglied dieser Rolle und besitzt dadurch alle Rechte, die für diese Rolle vergeben wurden.

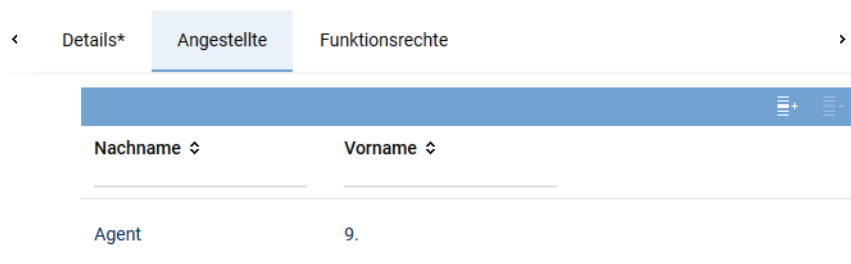



Abb. 94: Rollen-Modul - Registerkarte Angestellte



Im Angestellten-Modul können Sie den Umfang der Funktionsrechte, die einem Benutzer über eine Rolle zugewiesen wurden, mit individuellen Funktionsrechten ergänzen.

### 6.2.2.1 Benutzer zuordnen

1. Klicken Sie auf das Symbol  (*Hinzufügen*).

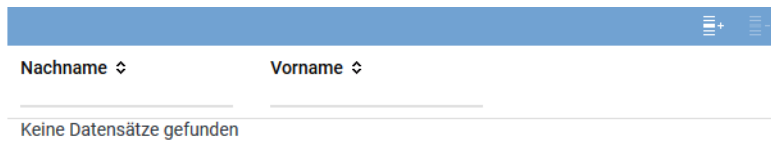
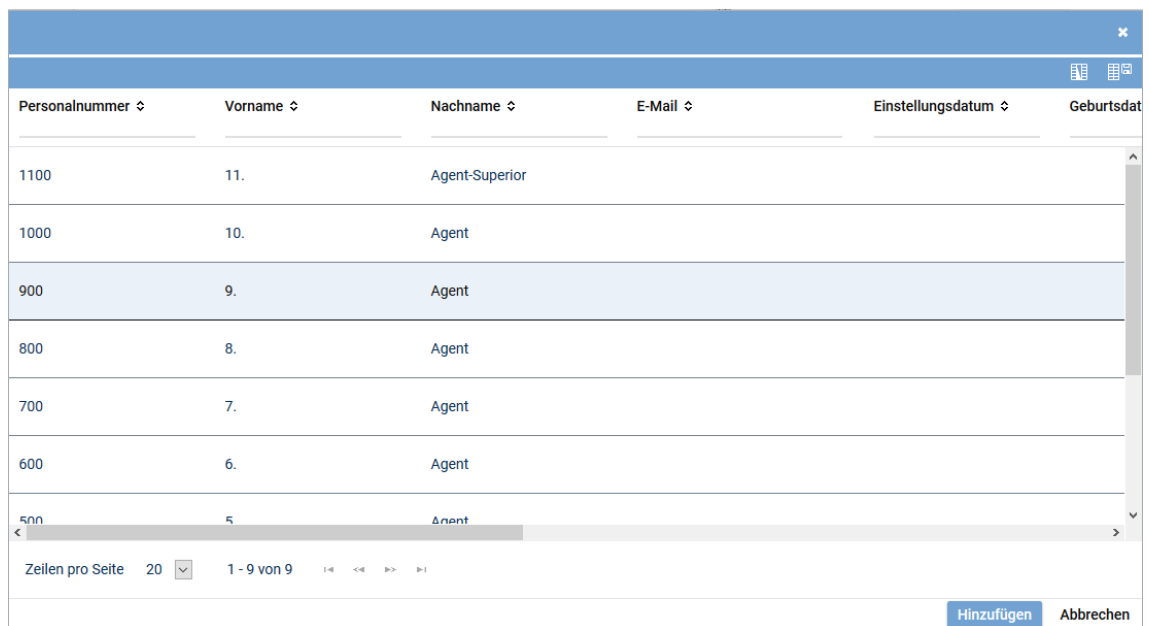


Abb. 95: Benutzer zuordnen

2. Wählen Sie einen oder mehrere Benutzer aus der Liste aus.  
Um mehrere Benutzer auszuwählen oder eine Auswahl zurückzunehmen, klicken Sie auf die entsprechende Zeile während Sie die [Strg]-Taste gedrückt halten.




Personalnummer	Vorname	Nachname	E-Mail	Einstellungsdatum	Geburtsdatum
1100	11.	Agent-Superior			
1000	10.	Agent			
900	9.	Agent			
800	8.	Agent			
700	7.	Agent			
600	6.	Agent			
500	5.	Agent			

Abb. 96: Benutzer hinzufügen

3. Um die ausgewählten Benutzer hinzuzufügen, klicken Sie auf die Schaltfläche *Hinzufügen*.  
Um die Auswahl zu verwerfen und das Fenster zu schließen, klicken Sie auf die Schaltfläche *Abbrechen*.

### 6.2.2.2 Benutzerzuordnung löschen

1. Wählen Sie den Benutzer, den Sie entfernen möchten, in der Liste aus und klicken Sie auf das Symbol  (*Entfernen*).

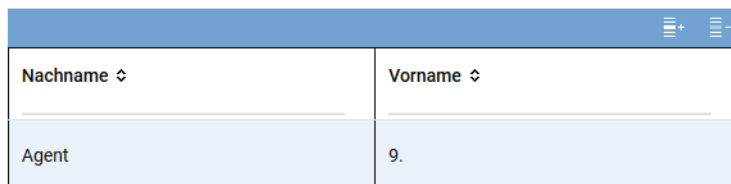


Abb. 97: Benutzerzuordnung löschen

### 6.2.3 Registerkarte Funktionsrechte

Hier können Sie die Funktionsrechte der Rolle anzeigen und zuordnen.

<	Details*	Angestellte	<b>Funktionsrechte</b>	>
System Configuration				▸
INSIGHTneo				▸
System Monitoring				▸

Abb. 98: Rollen-Modul - Registerkarte Funktionsrechte (Beispiel)

- Um die Funktionsrechte an einer Applikation anzupassen, öffnen Sie das Gruppenfeld mit dem entsprechenden Applikationsnamen.  
⇒ Alle Teilbereiche der Applikation werden aufgelistet.

System Configuration	▼
<input type="checkbox"/> Alle Funktionsrechte für System Configuration	
Benutzerkonfiguration	+
Mandanten	+

Abb. 99: Funktionsrechte - Teilbereiche anzeigen (Beispiel)

- Falls Sie dem Benutzer pauschal alle Funktionsrechte an einer Applikation zuweisen möchten, aktivieren Sie das Kontrollkästchen *Alle Funktionsrechte für ....* Dieses Recht ist übergeordnet und gilt für alle Module dieser Applikation.






Die Option, alle Funktionsrechte zu einer Applikation pauschal zuzuweisen, steht nicht für alle Applikationen zur Verfügung.

- Falls Sie die Funktionsrechte selektiv zuweisen möchten, öffnen Sie die Details zu einem Teilbereich (z. B. einem Modul), indem Sie auf das Symbol "+" in der Zeile mit dem entsprechenden Text klicken.  
⇒ Alle Funktionsrechte zu diesem Teilbereich werden eingeblendet.

System Configuration	▼
<input type="checkbox"/> Alle Funktionsrechte für System Configuration	
Benutzerkonfiguration	-
Name	Typ
<input type="checkbox"/> Darf Benutzer konfigurieren	+
Mandanten	+

Abb. 100: Funktionsrechte - Funktionsrechte anzeigen

(1. Spalte)	Zeigt an, ob das Funktionsrecht individuell zugewiesen wurde. <input checked="" type="checkbox"/> = individuelles Funktionsrecht <input type="checkbox"/> = kein individuelles Funktionsrecht
Name	Beschreibung des Funktionsrechts.


<i>Typ</i>	Zeigt an, welche Lizenz für dieses Recht benötigt wird.
	= Agenten-Lizenz
	= Supervisoren-Lizenz
	= Basis-Lizenz (ohne Agenten- oder Supervisoren-Rechte)

Tab. 4: Funktionsrechte

- Um alle Funktionsrechte für einen Teilbereich zuzuweisen, aktivieren Sie das entsprechende Kontrollkästchen *Alle Funktionsrechte am....*  
Um nur einzelne Funktionsrechte zuzuweisen, aktivieren Sie nur die Kontrollkästchen zu den Funktionsrechten, die Sie zuweisen möchten.
- Falls Sie die Details zu einem Teilbereich wieder ausblenden möchten, klicken Sie auf das Symbol "-" in der Zeile mit dem entsprechendem Text.

### 6.3

#### Neue Rolle anlegen

- Klicken Sie in der Symbolleiste auf das Symbol  (*Erstellen*).
- Nehmen Sie in den Registerkarten der Detailansicht alle Einstellungen vor, wie in den entsprechenden Kapiteln beschrieben (siehe [Kapitel "Detailansicht", S. 83](#)).  
Sie können dabei ohne Zwischenspeicherung zwischen den Registerkarten wechseln, ohne dass Ihre Einstellungen verloren gehen.
- Um nach der Beendigung der Eingaben die Einstellungen zu speichern, klicken Sie auf die Schaltfläche *Speichern*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Zurücksetzen*.

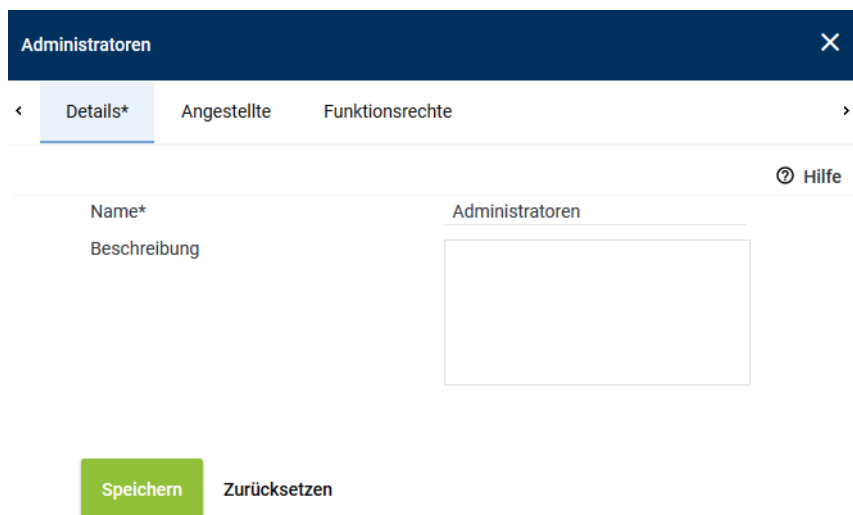


Abb. 101: Rolle speichern

### 6.4

#### Rolle duplizieren

- Wählen Sie in der Hauptansicht die Rolle aus, die Sie duplizieren möchten.
- Klicken Sie in der Symbolleiste auf das Menü *Rollen*.
- Wählen Sie eine der folgenden Optionen:

<i>Duplizieren mit Angestellten</i>	Legt eine Kopie der ausgewählten Rolle mit den zugeordneten Angestellten an.
<i>Duplizieren ohne Angestellte</i>	Legt eine Kopie der ausgewählten Rolle ohne die zugeordneten Angestellten an.

- In der Detailansicht wird eine Kopie der Rolle angelegt.

5. Geben Sie der kopierten Rolle einen neuen Namen.
6. Nehmen Sie in den Registerkarten der Detailansicht alle Einstellungen vor, wie in den entsprechenden Kapiteln beschrieben (siehe [Kapitel "Detailansicht", S. 83](#)). Sie können dabei ohne Zwischenspeicherung zwischen den Registerkarten wechseln, ohne dass Ihre Einstellungen verloren gehen.
7. Um nach der Beendigung der Eingaben die Einstellungen zu speichern, klicken Sie auf die Schaltfläche *Speichern*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Zurücksetzen*.

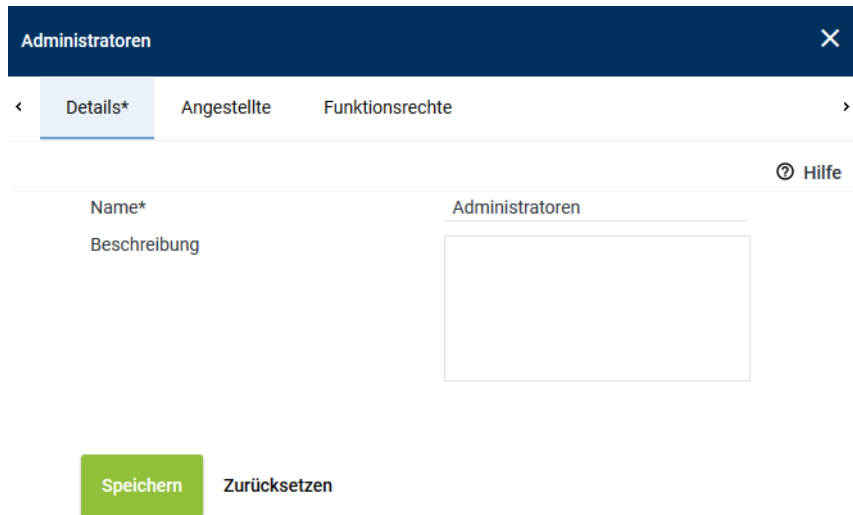


Abb. 102: Rolle speichern

## 6.5

### Rolle bearbeiten

1. Wählen Sie in der Hauptansicht die Rolle aus, die Sie bearbeiten möchten.
2. Nehmen Sie in den Registerkarten der Detailansicht alle notwendigen Änderungen vor (siehe [Kapitel "Detailansicht", S. 83](#)). Sie können dabei ohne Zwischenspeicherung zwischen den Registerkarten wechseln, ohne dass Ihre Einstellungen verloren gehen.
3. Um nach der Beendigung der Eingaben die Einstellungen zu speichern, klicken Sie auf die Schaltfläche *Speichern*.  
Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche *Zurücksetzen*.

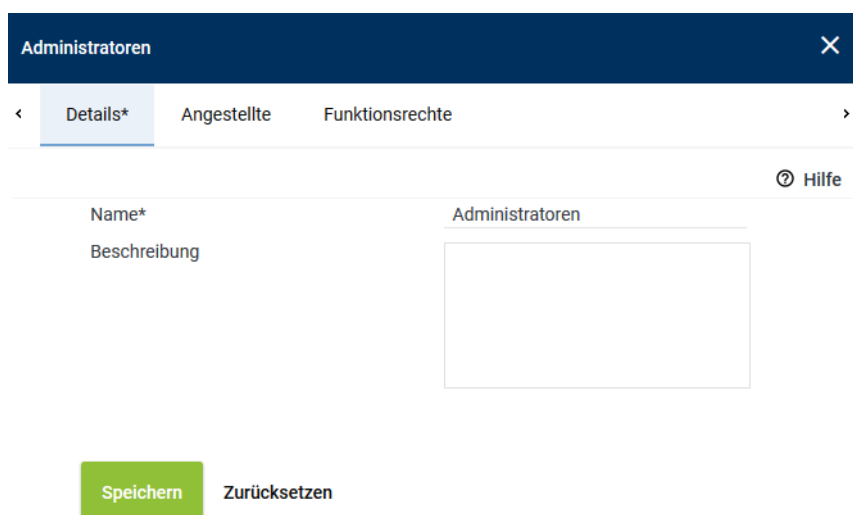



Abb. 103: Änderungen speichern



## 6.6

**Rolle löschen**

1. Wählen Sie in der Hauptansicht die Rolle aus, die Sie löschen möchten.
2. Klicken Sie in der Symbolleiste auf das Symbol  (Löschen).
3. Um die ausgewählte Rolle wirklich zu löschen, bestätigen Sie die Sicherheitsabfrage.

---

Das System erzeugt keine Meldung, falls die Rolle, die Sie löschen, noch einem Benutzer zugewiesen ist.



Der Benutzer verliert durch die Löschung der Rolle alle Funktionsrechte, die er über die Rolle erhalten hatte.

Wenn der Benutzer gerade am System angemeldet ist, wird die Löschung der Rolle erst wirksam, nachdem er sich vom System abgemeldet hat.

---

## 7

## Vordefinierte Funktionspakete

Für die Benutzer des Systembetreibers bietet das *neo*-System folgende vordefinierte Funktionspakete, die den Benutzern ausgewählte Funktionsrechte zur Verfügung stellen:

- **Superuser**

Ein Superuser besitzt alle Funktionsrechte im System, zu denen auch Lizenzen zur Verfügung stehen.

- **Superadmin**

Superadmin-Rechte sind nur in einer Cloud-Umgebung verfügbar und müssen bei Bedarf freigeschaltet werden.

Ein Superadmin besitzt eingeschränkte Superuser-Funktionsrechte im System.

Angestellte des Systembetreibers, die als Superadmin konfiguriert sind, können sich bei jedem im System vorhandenen Mandanten mit den Befugnissen eines Superusers dieses Mandanten anmelden.

## 7.1

## Superuser anlegen

1. Öffnen Sie das Angestellten-Modul.
2. Wählen Sie in der Hauptansicht den Benutzer aus, dem Sie Superuser-Rechte geben möchten.
3. Klicken Sie in der Detailansicht auf die Registerkarte *Einstellungen*.
4. Öffnen Sie das Gruppenfeld *Berechtigungen*.
5. Aktivieren Sie das Kontrollkästchen vor *Superuser*.

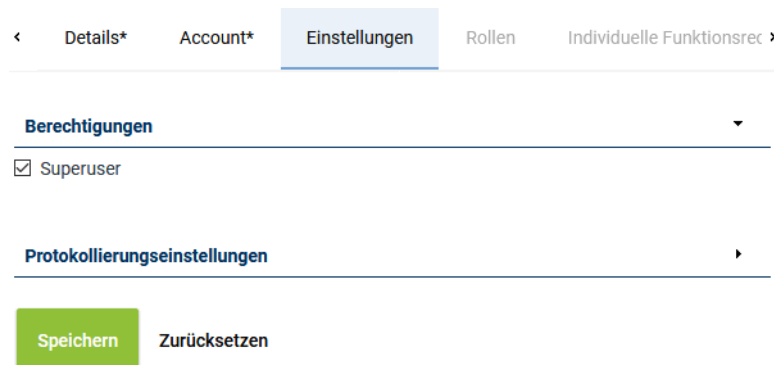


Abb. 104: Superuser anlegen

6. Klicken Sie auf die Schaltfläche *Speichern*, um die Einstellung zu speichern.

## 7.2

## Superadmin anlegen

1. Öffnen Sie das Angestellten-Modul.
2. Wählen Sie in der Hauptansicht den Benutzer aus, dem Sie Superadmin-Rechte geben möchten.
3. Klicken Sie in der Detailansicht auf die Registerkarte *Einstellungen*.
4. Öffnen Sie das Gruppenfeld *Berechtigungen*.
5. Aktivieren Sie das Kontrollkästchen vor *Superuser*.
6. Aktivieren Sie das Kontrollkästchen vor *Superadmin*.

**HINWEIS!** Die Option *Superadmin* wird nur angezeigt, wenn die entsprechende Lizenz im System vorhanden ist.

[Details\\*](#)

[Account\\*](#)

[Einstellungen](#)

[Rollen](#)

[Individuelle Funktionsrec](#)

**Berechtigungen** ▼☒ Superuser☒ Superadmin**Protokollierungseinstellungen** ▶

Abb. 105: Superadmin anlegen

7. Klicken Sie auf die Schaltfläche *Speichern*, um die Einstellung zu speichern.

## Abbildungsverzeichnis

Abb. 1	Mandanten-Modul - Hauptansicht .....	12
Abb. 2	Mandanten-Modul - Symbolleiste .....	12
Abb. 3	Mandanten-Modul - Detailansicht für den Mandanten "System" .....	13
Abb. 4	Mandanten-Modul - Detailansicht für normale Mandanten .....	15
Abb. 5	Mandanten-Modul - Detailansicht für Wiederverkäufer .....	16
Abb. 6	Mandanten-Modul - Detailansicht für normale Mandanten .....	17
Abb. 7	Zeitzone hinzufügen .....	18
Abb. 8	Tabellenansicht nach der Zeichenfolge ber gefiltert (Beispiel) .....	19
Abb. 9	Zeitzone hinzufügen .....	19
Abb. 10	Systemerreichbarkeit hinzufügen .....	20
Abb. 11	Systemerreichbarkeit konfigurieren .....	20
Abb. 12	Adresse hinzufügen .....	20
Abb. 13	Adresse hinzufügen .....	21
Abb. 14	Kontaktperson hinzufügen .....	21
Abb. 15	Kontaktperson hinzufügen .....	21
Abb. 16	Mandanten-Modul - Registerkarte Extensions .....	22
Abb. 17	Mandanten Extensions zuweisen .....	23
Abb. 18	Extensions entfernen .....	24
Abb. 19	Extensions auswählen .....	25
Abb. 20	Mandanten-Modul - Registerkarte PBX-Agenten-ID .....	26
Abb. 21	Mandanten PBX-Agenten-IDs zuweisen .....	27
Abb. 22	PBX-Agenten-IDs auswählen .....	28
Abb. 23	Mandanten-Modul - Registerkarte Chat-IDs .....	29
Abb. 24	Mandanten Chat-IDs zuweisen .....	30
Abb. 25	Chat-IDs auswählen .....	31
Abb. 26	Mandanten-Modul - Registerkarte Passwörter .....	32
Abb. 27	Passwortlänge festlegen .....	33
Abb. 28	Pflichtzeichen festlegen .....	33
Abb. 29	Passwortsicherheit konfigurieren .....	34
Abb. 30	Verbotene Passwörter festlegen .....	35
Abb. 31	Erweiterte Passworteinstellungen festlegen .....	36
Abb. 32	Listeneintrag bearbeiten .....	36
Abb. 33	Mandanten-Modul - Registerkarte Allgemeine Einstellungen .....	37
Abb. 34	Benutzerinaktivität konfigurieren .....	37
Abb. 35	SMTP-Account hinzufügen .....	38
Abb. 36	Gruppenfeld SNMP-Agent (Beispiele) .....	39
Abb. 37	Login-Einstellungen konfigurieren .....	41
Abb. 38	Sonstige Einstellungen konfigurieren .....	43
Abb. 39	Nutzungsbedingungen konfigurieren .....	44
Abb. 40	Mandanten-Modul - Registerkarte LDAP-Authentifizierung .....	45
Abb. 41	LDAP-Verbindungsdaten .....	45

Abb. 42	LDAP-Verbindungsdaten bearbeiten (Beispiel) .....	45
Abb. 43	Web-Service-Funktionen für den Systembetreiber .....	47
Abb. 44	Web-Service-Funktionen für den Mandanten .....	49
Abb. 45	Exportserver auswählen.....	51
Abb. 46	Server zuordnen.....	51
Abb. 47	Server auswählen (Beispiel) .....	52
Abb. 48	Web-Service-Funktionen für den Wiederverkäufer .....	53
Abb. 49	Mandanten-Modul - Registerkarte PBX .....	55
Abb. 50	PBX zuweisen .....	55
Abb. 51	PBX hinzufügen .....	56
Abb. 52	PCX-Zuweisung entfernen .....	56
Abb. 53	Registerkarte Systemlizenzen.....	57
Abb. 54	Mandanten-Modul - Hauptansicht (Beispiel) .....	58
Abb. 55	Mandanten speichern.....	59
Abb. 56	Änderungen speichern .....	60
Abb. 57	OAuth-Login aktivieren (Beispiel).....	61
Abb. 58	Angestellten-Modul - Hauptansicht .....	62
Abb. 59	Angestellten-Modul - Symbolleiste .....	63
Abb. 60	Zusammenfassung der Funktionsrechte .....	64
Abb. 61	Fenster Suchkriterien (Beispiel) .....	65
Abb. 62	Angestellten-Modul - Detailansicht .....	66
Abb. 63	Angestellten-Modul - Registerkarte Details .....	67
Abb. 64	Daten des Angestellten bearbeiten .....	68
Abb. 65	Bild hochladen.....	69
Abb. 66	Datei hochladen .....	69
Abb. 67	Bild entfernen (Beispiel) .....	70
Abb. 68	Adresse hinzufügen .....	70
Abb. 69	Adresse hinzufügen .....	70
Abb. 70	Datenschutz und Nutzungsbedingungen hinzufügen.....	71
Abb. 71	Datenschutz und Nutzungsbedingungen hinzufügen.....	71
Abb. 72	Angestellten-Modul - Registerkarte Account .....	71
Abb. 73	Account hinzufügen.....	72
Abb. 74	Authentifizierung via LDAP aktivieren .....	73
Abb. 75	Kombinationsbenutzer zuordnen .....	73
Abb. 76	Kombinationsbenutzer hinzufügen.....	74
Abb. 77	Kombinationsbenutzer-Zuordnung löschen .....	74
Abb. 78	Angestellten-Modul - Registerkarte Einstellungen .....	75
Abb. 79	Berechtigungen einstellen.....	75
Abb. 80	Protokollierung einstellen .....	76
Abb. 81	Angestellten-Modul - Registerkarte Rollen .....	76
Abb. 82	Rollen zuordnen .....	77
Abb. 83	Rolle hinzufügen .....	77

Abb. 84	Rollenzuordnung löschen .....	77
Abb. 85	Angestellten-Modul - Registerkarte Individuelle Funktionsrechte (Beispiel) .....	78
Abb. 86	Funktionsrechte - Teilbereiche anzeigen (Beispiel) .....	78
Abb. 87	Funktionsrechte - Funktionsrechte anzeigen .....	79
Abb. 88	Angestellten speichern .....	80
Abb. 89	Änderungen speichern .....	80
Abb. 90	Rollen-Modul - Hauptansicht.....	82
Abb. 91	Rollen-Modul - Symbolleiste .....	82
Abb. 92	Rollen-Modul - Detailansicht .....	83
Abb. 93	Rollen-Modul - Registerkarte Details .....	84
Abb. 94	Rollen-Modul - Registerkarte Angestellte.....	84
Abb. 95	Benutzer zuordnen.....	85
Abb. 96	Benutzer hinzufügen .....	85
Abb. 97	Benutzerzuordnung löschen .....	85
Abb. 98	Rollen-Modul - Registerkarte Funktionsrechte (Beispiel).....	86
Abb. 99	Funktionsrechte - Teilbereiche anzeigen (Beispiel) .....	86
Abb. 100	Funktionsrechte - Funktionsrechte anzeigen .....	86
Abb. 101	Rolle speichern .....	87
Abb. 102	Rolle speichern .....	88
Abb. 103	Änderungen speichern .....	88
Abb. 104	Superuser anlegen.....	90
Abb. 105	Superadmin anlegen .....	91

## Tabellenverzeichnis

Tab. 1	Login-Daten - Systembetreiber .....	7
Tab. 2	Login-Daten - 1. Mandant .....	7
Tab. 3	Funktionsrechte.....	79
Tab. 4	Funktionsrechte.....	86

## Glossar

### CSV

Comma-separated values ist ein Dateiformat, das den Aufbau einer Textdatei zur Speicherung oder zum Datenaustausch beschreibt.

### G.729A

G.729 Annex A ist ein Codec zur Komprimierung von Sprache in digitale Signale mit geringerer Komplexität, Festkomma-Arithmetik und einer Datenrate von 8 Kbit/s.

### IP

Internet Protocol, Basisprotokoll für die Internetkommunikation

### LDAP

Lightweight Directory Access Protocol

### MIB

Management Information Base; Datei, in der die zur Verfügung gestellten SNMP-Objekte definiert werden.

### PBX

Private Branch Exchange, Telefonanlage

### SMTP

Simple Mail Transfer Protocol ist ein Protokoll, das zum Senden von E-Mails in Computernetzen dient.

### SNMP

Simple Network Management Protocol ist ein Netzwerkprotokoll und dient zur Überwachung und Steuerung von Netzwerkkomponenten. Das Protokoll ist beim Transport nicht auf das IP-Netzwerkprotokoll angewiesen. Es versendet unaufgefordert Nachrichten (Traps) von Aktivitäten auf den Netzwerkelementen.

### SSL

Secure Socket Layer

### SSO

Single Sign On; Vereinfachtes Login-Verfahren. Nach einer einmaligen Authentifizierung an einem Arbeitsplatz kann der Benutzer an diesem Arbeitsplatz alle Dienste und Applikationen nutzen, für die er autorisiert ist. Er muss sich an den einzelnen Applikationen nicht erneut authentifizieren.

### TLS

Transport Layer Security; Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt.



---

### **URL**

Uniform Resource Locator. Identifiziert und lokalisiert eine Ressource (z. B. eine Website) über die zu verwendende Zugriffsmethode (z. B. das verwendete Netzwerkprotokoll wie HTTP oder FTP) und den Ort der Ressource in Computernetzwerken. (Quelle: Wikipedia 20.11.2013)

### **WSDL**

Web Service Description Language; Metasprache, mit deren Hilfe die angebotenen Funktionen, Daten, Datentypen und Austauschprotokolle eines Webservice beschrieben werden können. (Quelle: Wikipedia 12.12.2014)

### **XML**

Extensible Markup Language ist eine erweiterbare Auszeichnungssprache zur Beschreibung und dem Austausch von Datenstrukturen.