

NUTZERHANDBUCH

TI-MESSENGER ORG-ADMIN CLIENT

Deutsche Telekom Healthcare and Security Solutions GmbH

Version 2.2

Stand 22.01.2026

Inhalt

1	Einleitung	4
2	Anmeldung	4
3	Funktionen	6
3.1	<i>Benutzerverwaltung</i>	6
3.1.1	Nutzerliste	6
3.1.2	Einzelne Nutzer	7
3.1.3	Benutzer	8
3.1.4	Geräte	9
3.1.5	Räume	10
3.1.6	IDP	11
3.2	<i>Raumverwaltung</i>	12
3.2.1	Raumverwaltung: Mitglieder	13
3.2.2	Raumverwaltung: Broadcast	14
3.3	<i>Gesundheitsdienste</i>	15
3.3.1	Allgemein	17
3.3.2	Endpunkte	18
3.3.3	Öffnungszeiten	19
3.3.4	Abwesenheiten	20
3.3.5	Spezialzeiten	21
3.3.6	Kontaktdaten	22
3.4	<i>Gesundheitsdienst erstellen</i>	23
3.4.1	Allgemeine Informationen	24
3.4.2	Endpunkte	25
3.4.3	Öffnungszeiten	26
3.4.4	Kontaktdaten	27
3.4.5	Zusammenfassung	28
3.5	<i>Organisationsinformationen</i>	29
3.6	<i>Benutzer erstellen</i>	30
3.7	<i>Broadcast</i>	31
3.8	<i>Medien</i>	32
3.9	<i>Meldungen</i>	35
3.9.1	Grundlegend	36

3.9.2	Detailinformationen.....	37
4	Absprung: KeyCloak	38
4.1	<i>KeyCloak: Users</i>	38
4.2	<i>KeyCloak: Neue User anlegen.....</i>	40
4.3	<i>KeyCloak: Groups.....</i>	42
4.4	<i>KeyCloak: Ausgewählte Gruppe.....</i>	43
4.5	<i>KeyCloak: Detailinformationen User.....</i>	46
4.5.1	KeyCloak: User Credentials	48
4.5.2	KeyCloak: User Role mapping	50
4.5.3	KeyCloak: User Groups.....	52
4.5.4	KeyCloak: User Consents.....	54
4.5.5	KeyCloak: User Sessions.....	55
4.6	<i>KeyCloak: Einstellungen zum eigenen User</i>	57
4.6.1	KeyCloak: Manage account – Personal info	58
4.6.2	KeyCloak: Manage account – Signing in.....	59
4.6.3	KeyCloak: Manage account – Device Activity.....	60
4.6.4	KeyCloak: Manage account – Linked accounts.....	61
4.6.5	KeyCloak: Manage account – Applications	62
5	Mein Account.....	63
5.1	<i>Einstellungen</i>	64
5.1.1	Einstellungen: Allgemein.....	64
5.1.2	Passwort ändern	65
5.1.3	Einstellungen: Sicherheit.....	66
5.1.4	Einstellungen: Info	67
5.1.5	Einstellungen: Impressum.....	68
5.1.6	Einstellungen: Datenschutz.....	69
5.2	<i>Ausloggen.....</i>	70
6	Passwortanforderungen.....	71
7	Änderungshistorie.....	73

1 Einleitung

Dieses Nutzerhandbuch bietet eine umfassende Anleitung zur Nutzung des TI-Messengers für die Administratoren. Entwickelt von der Deutschen Telekom Healthcare and Security Solutions GmbH, deckt es alle wesentlichen Funktionen und Prozesse ab, die für eine effektive Kommunikation im Gesundheitswesen erforderlich sind.

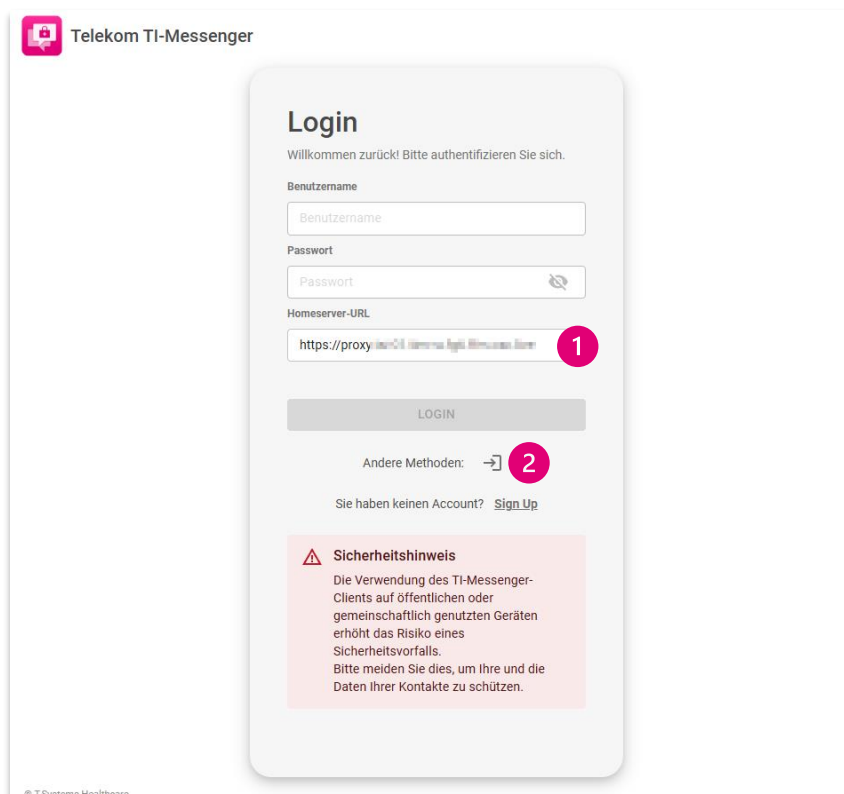
Das Handbuch dient als wertvolle Ressource, um Administratoren bei der effizienten Verwaltung der Plattform zu unterstützen. Sie finden hier detaillierte Informationen zur Benutzer- und Berechtigungsverwaltung, zur Überwachung der Systemaktivitäten sowie zur Handhabung von Fehlermeldungen und technischen Problemen.


Ziel dieses Handbuches ist es, Ihnen alle notwendigen Werkzeuge und Kenntnisse zur Verfügung zu stellen, um den TI-Messenger optimal zu nutzen und die Qualität der internen sowie externen Kommunikation in der Organisation zu fördern.

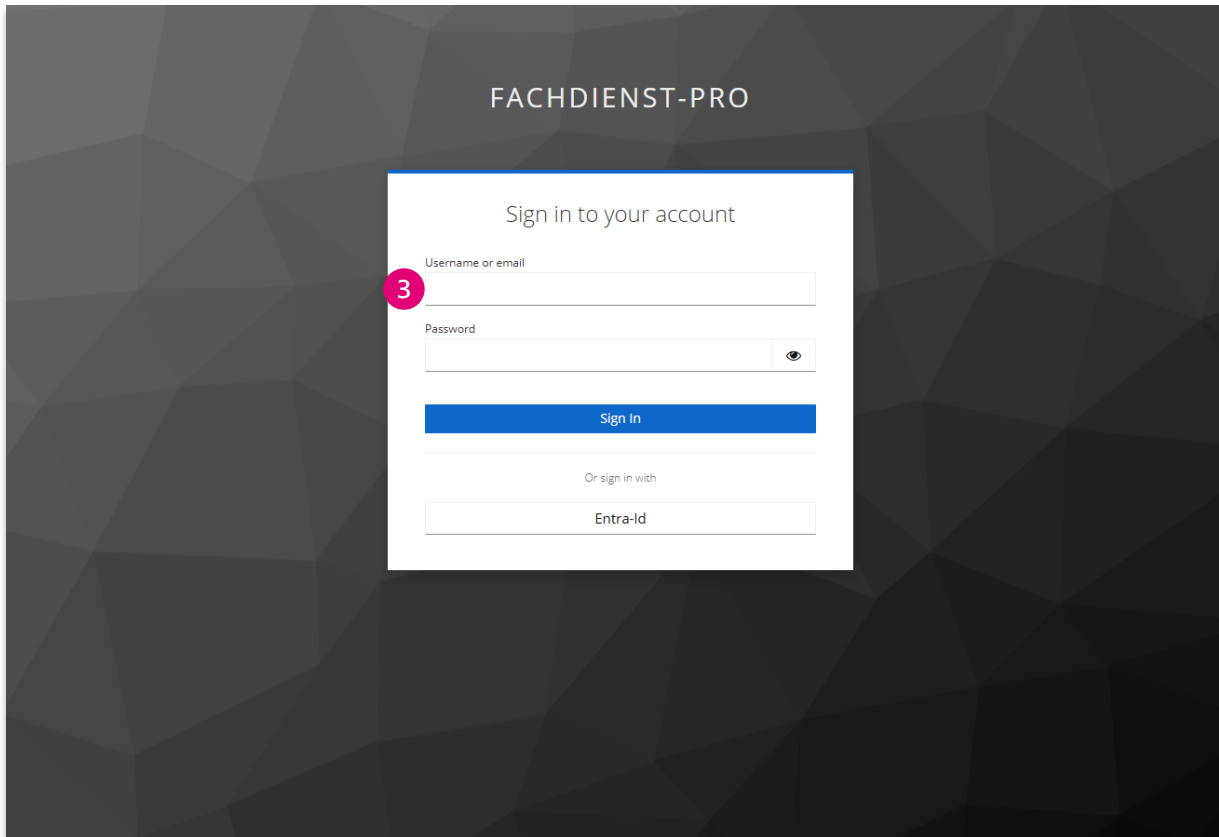
2 Anmeldung

Die Anmeldung an der Administrationsoberfläche des TI-Messengers ist der erste Schritt, um Zugang zu den umfassenden Verwaltungsfunktionen zu erhalten, die für die effektive Nutzung der Plattform erforderlich sind.

Der Link, über den Sie auf die Administrationsoberfläche des TI-Messengers zugreifen können, wurde Ihnen in per Email bereitgestellt. Dort öffnet sich die Anmeldemaske, in die Sie Ihre Zugangsdaten eingeben können.



- 1 Für die Anmeldung benötigen Sie im ersten Schritt die Homeserver-URL. Bitte geben Sie diese im Feld [**Homeserver-URL**] an.
- 2 Wenn Sie die Homeserver-URL angegeben haben, öffnet sich unter dem Login Button ein neues Feld [**Andere Methoden**]. Klicken Sie bitte auf das Symbol . Sie werden zum Login über KeyCloak geleitet.



- 3 Anschließend geben Sie in die Anmeldemaske von KeyCloak Ihren **Usernamen** oder **E-Mail-Adresse** sowie das **Passwort** zu Ihrem Account ein. Klicken Sie zuletzt auf den Button [**Sign In**].

Nach der korrekten Eingabe Ihrer Daten gelangen Sie zur Benutzeroberfläche des Org-Admin-Clients.

Hinweis: Zur Nutzung eines anderen Authentifizierungsverfahren als mitgeliefert siehe Kapitel 3.5.

3 Funktionen

Im folgenden Kapitel werden die Funktionen des Org-Admin-Clients des TI-Messengers detailliert beschrieben, um Ihnen als Administrator alle notwendigen Werkzeuge zur Verfügung zu stellen, die Sie für die effektive Verwaltung Ihrer Benutzer und Chaträume benötigen. Sie erfahren, wie Sie Benutzerprofile anlegen und verwalten, Räume organisieren, Gesundheitsdienste konfigurieren und Kommunikationsstrukturen optimieren können. Zudem werden Sie in die Lage versetzt, die Nutzung von Medien zu überwachen und etwaige Meldungen zu verwalten, um sicherzustellen, dass die Plattform sowohl sicher als auch benutzerfreundlich bleibt.

3.1 Benutzerverwaltung

In der Benutzerverwaltung erhalten Sie als Org-Admin einen umfassenden Überblick über alle Aspekte der Nutzerverwaltung im TI-Messenger. Dieses Kapitel erläutert, wie Sie die Nutzerliste einsehen, Benutzerprofile anlegen und anpassen, Geräte verwalten sowie Räume und Identitäten der Nutzer effektiv koordinieren können. Ziel ist es, Ihnen die notwendigen Werkzeuge und Informationen zur Verfügung zu stellen, um die Benutzer und deren Interaktionen innerhalb Ihrer Organisation optimal zu steuern und eine sichere, reibungslose Nutzung der Plattform zu gewährleisten.

Im Folgenden werden die Liste der Nutzer sowie die Funktionen auf der Seite der Benutzerverwaltung erläutert.

3.1.1 Nutzerliste

Avatar	Benutzer-ID	Anzeigename	Administrator	Deaktiviert	Erstellungszeitpunkt
	@orgadmin.orgadmin	orgadmin.orgadmin	Ja	Nein	18.09.2025, 14:56:16
	@orgadmin.orgadmin	orgadmin.orgadmin	Nein	Nein	29.09.2025, 13:02:31
	@orgadmin.orgadmin	orgadmin.orgadmin	Ja	Nein	09.09.2025, 11:59:43
	@orgadmin.orgadmin	orgadmin.orgadmin	Ja	Nein	03.12.2025, 14:02:51
	@orgadmin.orgadmin	orgadmin.orgadmin	Nein	Nein	16.09.2025, 08:41:24
	@orgadmin.orgadmin	orgadmin.orgadmin	Nein	Nein	27.10.2025, 14:33:53
	@orgadmin.orgadmin	orgadmin.orgadmin	Ja	Nein	15.08.2025, 11:19:15
	@orgadmin.orgadmin	orgadmin.orgadmin	Nein	Nein	21.10.2025, 08:22:15
	@orgadmin.orgadmin	orgadmin.orgadmin	Nein	Nein	11.09.2025, 13:25:18
	@orgadmin.orgadmin	orgadmin.orgadmin	Ja	Nein	04.09.2025, 15:37:40

1 In der **[Benutzerverwaltung]** erhalten Sie Zugriff auf eine umfassende Liste aller Benutzer, die auf Ihrem Homeserver registriert sind oder waren. Diese Liste enthält die folgenden Informationen:

- **Avatar:** Aktuelles Profilbild des Benutzers;
- **Benutzer-ID:** Endpunkt des Benutzers in der Form @[Username]:[Homeserver];
- **Anzeigename:** Aktueller Anzeigename des Benutzers;

- **Administrator:** Angabe darüber, ob der jeweilige Benutzer Admin-Rechte hat;
- **Deaktiviert:** Angabe darüber, ob das Benutzerprofil deaktiviert ist;
- **Erstellungszeitpunkt:** Tages- und Zeitangabe der Erstellung des Benutzerprofils.

- 2 Um gezielt nur alle Benutzer mit Administratorrechten anzuzeigen, klicken Sie auf den Reiter **[Administratoren]**.
- 3 Die Benutzerliste ist standardmäßig alphabetisch absteigend nach Benutzer-ID sortiert, erkennbar an dem Pfeilsymbol. Mit einem **Klick** auf eine der grauhinterlegten **Spaltenüberschriften** sortieren Sie die Liste alpha-numerisch absteigend nach der entsprechenden Spalte. Mit einem zweiten Klick auf die jeweilige Spaltenüberschrift kehren Sie die Sortierung um.
- 4 Wenn Sie einen neuen Benutzer hinzufügen möchten, klicken Sie auf **[Benutzer erstellen]**. Detaillierte Schritte hierzu finden Sie in Kapitel 3.6.
- 5 Darüber hinaus können Sie über die Funktion **[Exportieren (CSV)]** eine vollständige Liste der Benutzerinformationen im CSV-Dateiformat herunterladen.
- 6 Ein **Klick** auf eine spezifische **Zeile** in der Tabelle öffnet das Benutzerprofil des gewählten Users. Für Anleitungen zur Bearbeitung und Interaktion mit den Profilen folgen Sie bitte den nachfolgenden Unterkapiteln.
- 7 Um einen bestimmten Benutzer schnell zu finden, nutzen Sie das Suchfeld **[Anzeigename suchen]**.

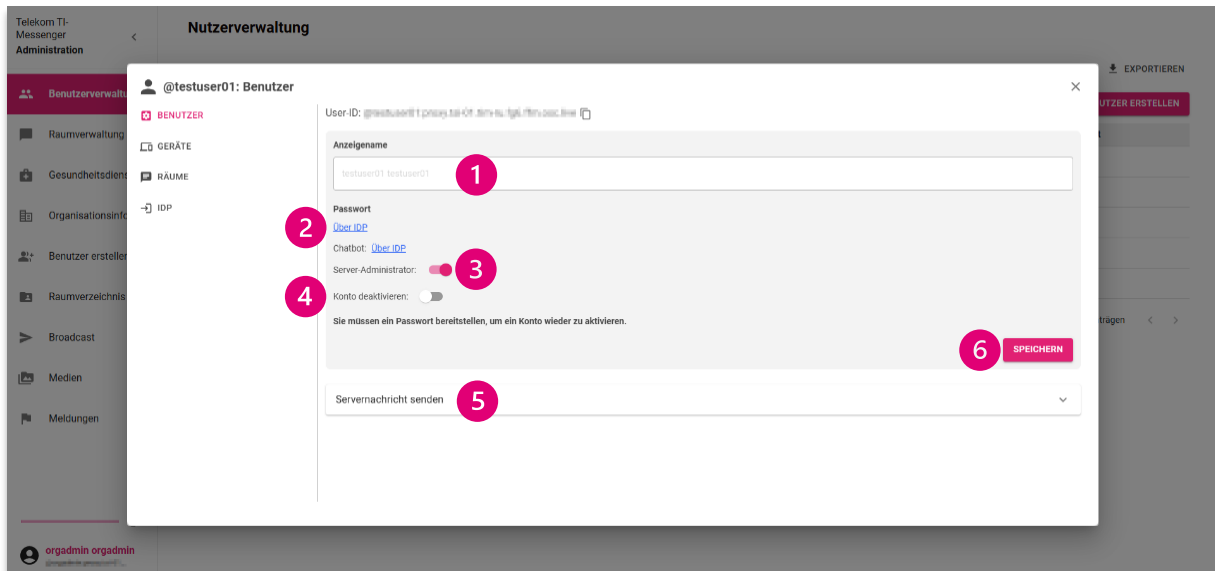
3.1.2 Einzelne Nutzer

Das Bearbeiten einzelner Nutzeraccounts ermöglicht es Administratoren, spezifische Informationen und Einstellungen der Benutzerprofile bei Bedarf anzupassen. Diese flexible Funktion umfasst die Änderung von Anzeigenamen, Passwörtern und Administrationsrechten sowie die Möglichkeit, Geräte zu löschen oder alle aktiven Räume anzuzeigen. Durch das gezielte Anpassen von Nutzerinformationen können Administratoren sicherstellen, dass die Benutzerprofile stets aktuellen Anforderungen entsprechen und die Sicherheit sowie die Benutzererfahrung im TI-Messenger optimiert werden. In diesem Abschnitt erfahren Sie, wie Sie die Profile einzelner Nutzer effektiv bearbeiten.

Wählen Sie aus der Nutzerliste ein einzelnes Profil aus und öffnen Sie dieses mit einem Klick. Es öffnet sich ein Fenster, in dem über die Sidebar vier verschiedene Bereiche ausgewählt werden können. Diese werden in den folgenden Unterkapiteln erläutert.

3.1.3 Benutzer

Die Möglichkeit, einzelne Nutzeraccounts zu bearbeiten, ist entscheidend für die Verwaltung der Benutzerprofile im TI-Messenger und ermöglicht es Ihnen, Anpassungen effizient vorzunehmen, um den spezifischen Anforderungen Ihrer Organisation gerecht zu werden.



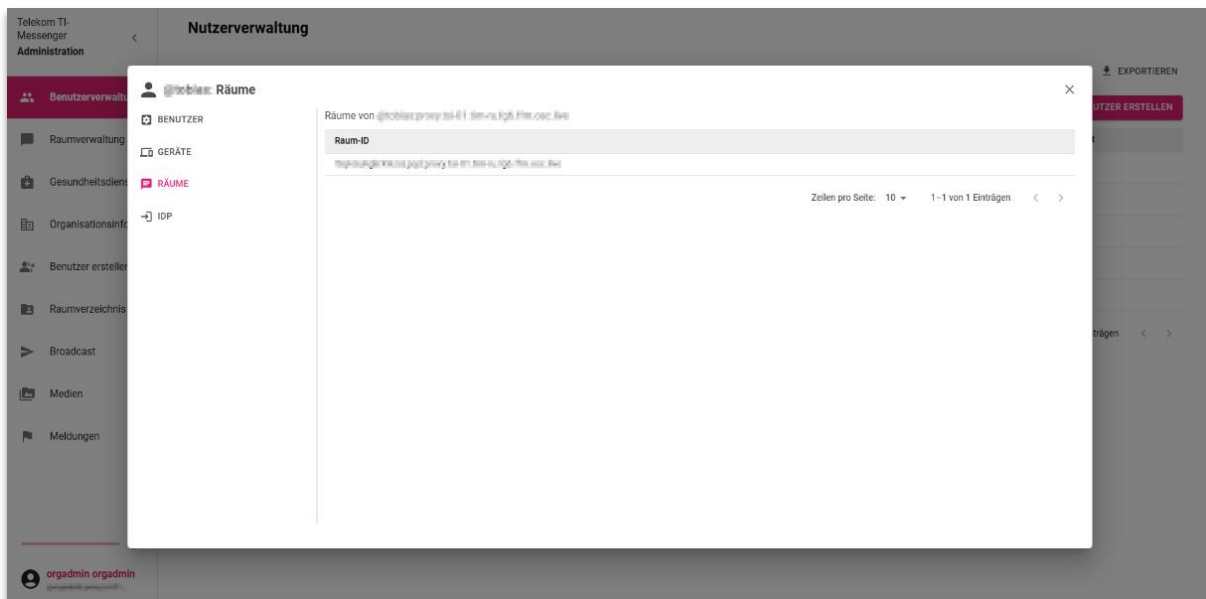
- 1 Über das Textfeld können Sie den Anzeigenamen des Benutzers ändern. Geben Sie hierzu einen neuen Namen in das **[Textfeld]** ein.
- 2 Sie haben die Möglichkeit, über den Absprung **[Über IDP]** das Passwort zu ändern.
- 3 Durch den Einsatz eines **Schiebereglers** können Sie einfach steuern, ob ein Benutzer **Administratorrechte** erhält. Wenn der Schieberegler aktiviert ist, hat der Benutzer Zugriff auf erweiterte Verwaltungsfunktionen im TI-Messenger, während bei Deaktivierung diese Rechte entzogen werden. Diese flexible Einstellung ermöglicht eine schnelle Anpassung der Berechtigungen je nach den Anforderungen Ihrer Organisation.
- 4 Mit einem **Schieberegler** können Sie ein **Benutzerkonto deaktivieren**. Wenn der Schieberegler aktiviert ist, wird das Konto des Benutzers deaktiviert, wodurch der Zugriff auf den TI-Messenger und alle damit verbundenen Funktionen unterbunden wird. Bei Deaktivierung des Schieberegler wird das Konto wieder aktiviert, sodass der Benutzer erneut auf die Plattform zugreifen kann. Bitte beachten Sie, dass Sie ein neues Passwort bereitstellen müssen, wenn Sie ein Konto wieder aktivieren möchten.

- 1 Um das Gerät eines Benutzers zu löschen, klicken Sie auf **[Gerät löschen]**.
- 2 Wenn Sie beispielsweise alle Geräte eines Benutzers löschen wollen, klicken Sie auf den Button **[Alle Geräte löschen]**. Dies ist unter anderem der Fall, wenn ein Sicherheitsverstoß aufgetreten ist und Sie alle laufenden Sitzungen auf dem Homeserver auf einmal schließen möchten. Alle dehydrierten Geräte werden damit auch gelöscht, d. h. User können bis zum erneuten Login keine Push-Nachrichten mehr erhalten.

Hinweis: Wenn ein Benutzer noch nicht die Erstanmeldung durchgeführt hat, bleibt die Liste unter **[Geräte]** leer. Sobald der Benutzer jedoch sein Profil eingerichtet hat, wird dort mindestens ein sogenanntes „**Dehydrated Device**“ angezeigt. Dieses Gerät ermöglicht den Empfang von Nachrichten für das Profil, auch wenn keine aktive Sitzung besteht.

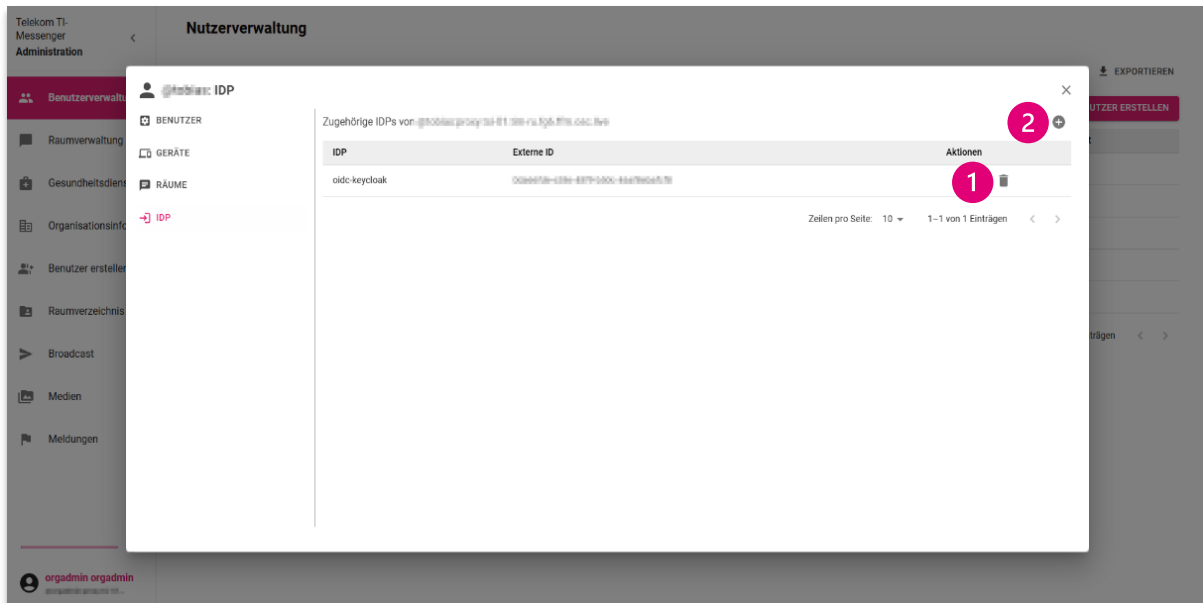
3.1.5 Räume

Unter **[Räume]** finden Sie alle Räume, in denen der jeweilige Nutzer Mitglied ist, mit Angabe der Raum-ID. Diese Liste dient Ihnen ausschließlich zur Übersicht.



3.1.6 IDP

Ein Identity Provider (IDP) ermöglicht die zentrale Verwaltung von Nutzeridentitäten und Zugriffsrechten. Sie erhalten eine Übersicht zu den IDPs eines Benutzers.



- 1 Wenn Sie eine IDP eines Benutzers löschen möchten, klicken Sie auf das Mülleimer-Symbol in der Spalte **Aktionen**.
- 2 Möchten Sie einen neuen IDP hinzufügen, klicken Sie auf das **Plus-Symbol**.

Hinweis: Wenn Sie ein Benutzerkonto deaktivieren, erhält der Benutzer bei seinem nächsten Anmeldeversuch die Fehlermeldung „Passwort oder Benutzername falsch“. Um ein deaktiviertes Konto wieder zu reaktivieren, müssen Sie zunächst ein neues Passwort festlegen und dieses dem Benutzer mitteilen. Der Benutzer muss dann den Erstanmeldevorgang erneut durchlaufen, wobei er seine unveränderte Benutzer-ID und das neue Initialpasswort eingibt.

Zusätzlich wird bei der Reaktivierung ein neuer Sicherheitsschlüssel generiert, da alle zuvor erstellten Sicherheitsschlüssel aufgrund der Kontodeaktivierung ihre Gültigkeit verlieren. Es ist wichtig zu beachten, dass ein Benutzer nach einer Kontodeaktivierung nicht mehr auf seine vorherigen Chats zugreifen kann.

Ein Raum kann maximal so viele Mitglieder haben, wie User auf dem Homeserver registriert sind;

- **Verschlüsselt:** Anzeige über den Verschlüsselungsstatus eines Raumes. Alle Räume im TI-Messenger sind verschlüsselt;
- **Sichtbarkeit:** Anzeige über den Sichtbarkeitsstatus eines Raumes. Alle Räume im TI-Messenger werden einem Org-Admin-User als „Privat“ angezeigt.

2 Um einen Raum zu löschen, klicken Sie auf das **Mülltonnensymbol** in der Spalte **Aktionen**.

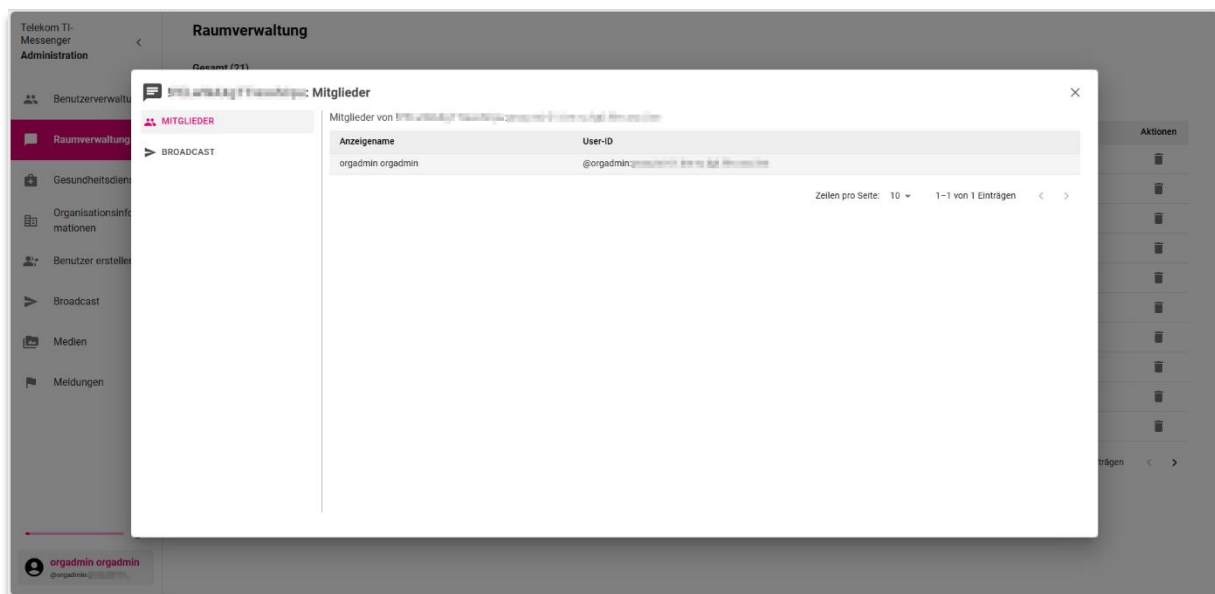
3 Die Liste ist standardmäßig alphabetisch absteigend nach Raumname sortiert, erkennbar an dem Pfeilsymbol. Mit einem **Klick** auf eine der grauhinterlegten **Spaltenüberschriften** sortieren Sie die Liste alpha-numerisch absteigend nach der entsprechenden Spalte. Mit einem zweiten Klick auf die jeweilige Spaltenüberschrift kehren Sie die Sortierung um.

4 Sie haben die Möglichkeit, über das Suchfeld [**Raumname / Raum-ID**] in der oberen linken Ecke nach einzelnen Räumen zu suchen. Sie können nicht nach Raum-Erstellern suchen.

5 Klicken Sie auf eine einzelne Zeile in der Tabelle, haben Sie Zugriff auf weitere Detailinformationen des jeweiligen Raumes. Sie haben beispielsweise einen Überblick über die Mitglieder des Raumes sowie die Möglichkeit Broadcast-Nachrichten zu verschicken. Weitere Informationen entnehmen Sie den nachfolgenden Kapiteln.

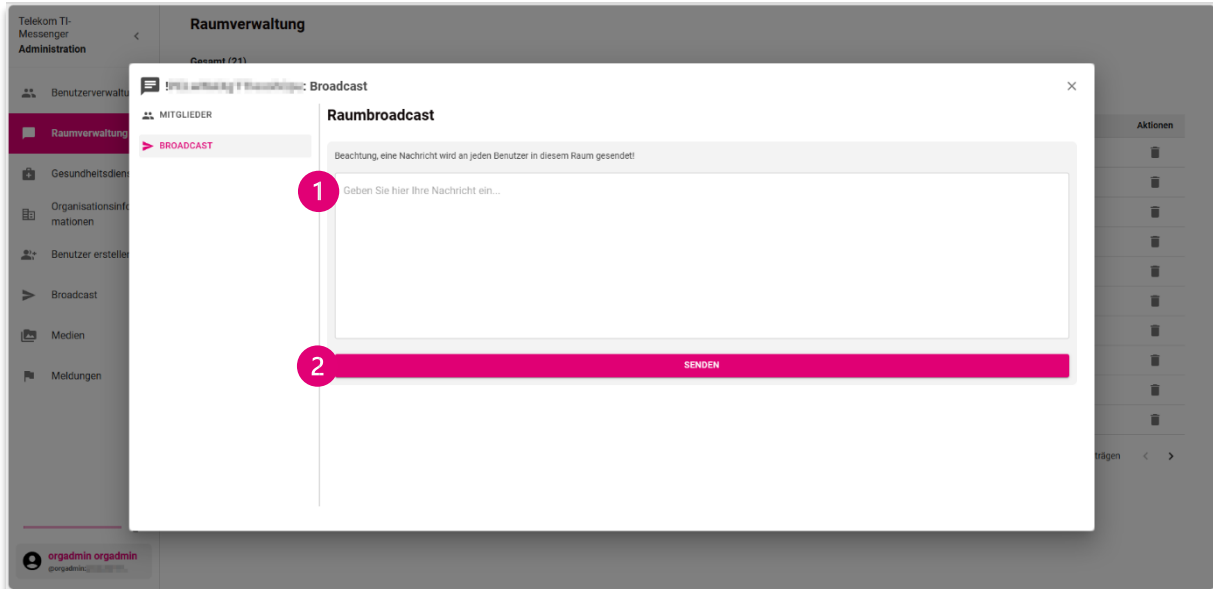
3.2.1 Raumverwaltung: Mitglieder

Unter [**Mitglieder**] finden Sie eine Übersicht darüber, welche Mitglieder sich in einem Raum befinden. Hier können Sie die Anzeigenamen und die TI-Messenger-IDs der Raummitglieder einsehen. Diese Liste dient Ihnen ausschließlich zur Übersicht.



3.2.2 Raumverwaltung: Broadcast

Der Reiter **[Broadcast]** bietet Ihnen die Möglichkeit, Broadcast-Nachrichten zu versenden und wichtige Informationen schnell und unkompliziert an alle Mitglieder eines Raumes zu übermitteln. Sie sorgen für eine einheitliche Informationsverteilung, ohne dass einzelne Nachrichten manuell versendet werden müssen, und verbessern so die Effizienz der internen Kommunikation.



- 1 Verfassen Sie eine Nachricht im Feld **[Geben Sie hier Ihre Nachricht ein...]**.
- 2 Klicken Sie abschließend auf **[Senden]**.

Nun wurde eine Nachricht an alle Mitglieder in dem ausgewählten Raum versendet.

3.3 Gesundheitsdienste

In diesem Kapitel erhalten Sie einen umfassenden Überblick über alle Gesundheitsdienste, die auf Ihrem Homeserver eingerichtet sind oder waren. Hier finden Sie wichtige Informationen zu jedem Dienst, darunter Name, Öffnungszeiten, Ausnahmen sowie die Sprachen, in denen der Dienst kommuniziert. Die Übersicht ermöglicht es Ihnen, Gesundheitsdienste effizient zu verwalten, indem Sie die spezifischen Details zu jedem Dienst einsehen und anpassen können.

Name	Öffnungszeiten	Ausnahmen	Sprachen	Endpunkte	Aktionen
Organisationseintrag	Keine Öffnungszeiten angegeben	Keine Ausnahmen angegeben	Keine Sprachen angegeben	Keine Endpunkte angegeben	
...	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch	@[User-ID]:[Homeserver]	
...	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch Englisch	@[User-ID]:[Homeserver]	
...	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Englisch	@[User-ID]:[Homeserver]	
...	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch	@[User-ID]:[Homeserver]	
...	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch Englisch	@[User-ID]:[Homeserver]	
...	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch	@[User-ID]:[Homeserver]	

1 Unter **[Gesundheitsdienste]** finden Sie alle Gesundheitsdienste, die auf Ihrem Homeserver angelegt sind oder waren. Die Liste enthält die folgenden Informationen:

- **Name:** Name des Gesundheitsdienstes;
- **Öffnungszeiten:** Öffnungszeiten des Gesundheitsdienstes. Wird ein Wochentag hier nicht aufgelistet, hat der Gesundheitsdienst an diesem Tag durchgängig geschlossen;
- **Ausnahmen:** Freitext-Angabe über Ausnahmen von den Öffnungszeiten, z. B. Angabe über Mittagspausen oder Feiertagsregelungen;
- **Sprachen:** Die von einem Gesundheitsdienst in der Kommunikation verwendeten Sprachen;
- **Matrix-ID:** ID der Benutzer, die als Endpoint für den Gesundheitsdienst zugeordnet wurden, in der Form „@[User-ID]:[Homeserver]“;
- **Aktionen:** Möglichkeit zum Löschen eines Gesundheitsdienstes. Klicken Sie dafür auf das Mülleimersymbol.

2 Sie haben die Möglichkeit, über das **Suchfeld [Gesundheitsdienst suchen...]** in der oberen linken Ecke nach einzelnen Gesundheitsdiensten zu suchen. Sie können nur nach Gesundheitsdienst-Namen, nicht nach konkreten Endpunkten suchen.

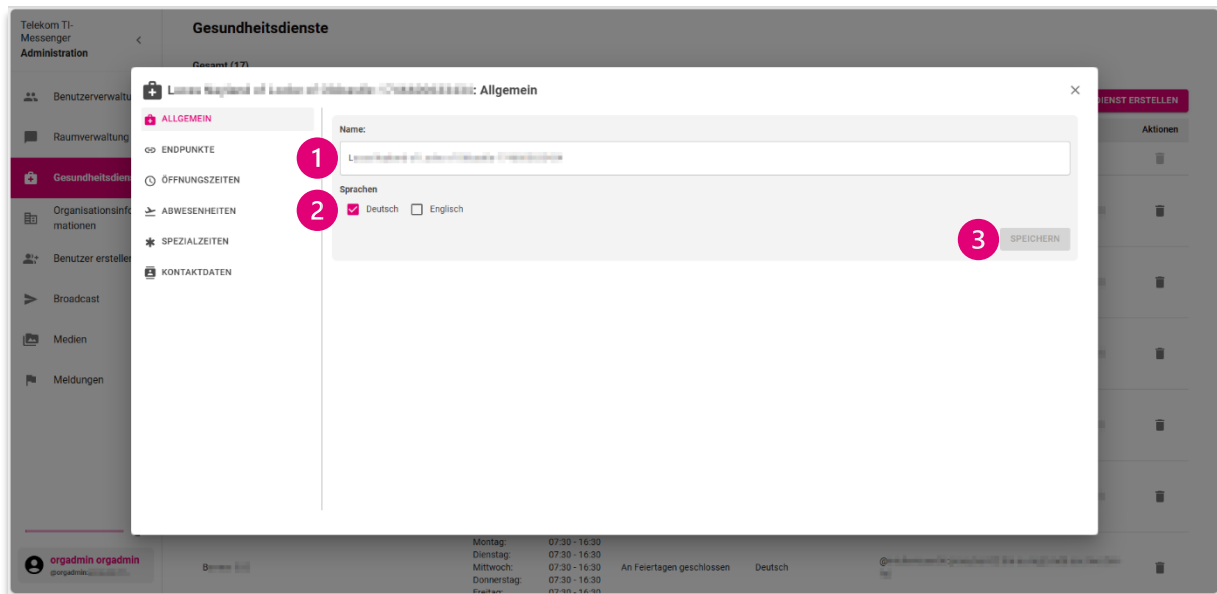
3 Über den Button **[Gesundheitsdienst erstellen]** können Sie einen neuen Gesundheitsdienst anlegen. Eine detaillierte Anleitung dazu finden Sie in Kapitel 3.4.

4

Klicken Sie auf eine einzelne **Zeile** in der Tabelle, haben Sie Zugriff auf weitere Detailinformationen über den jeweiligen Gesundheitsdienst. Es öffnet sich ein zusätzliches Fenster mit weiteren Optionen. Diese werden in den nachfolgenden Unterkapiteln erläutert.

3.3.1 Allgemein

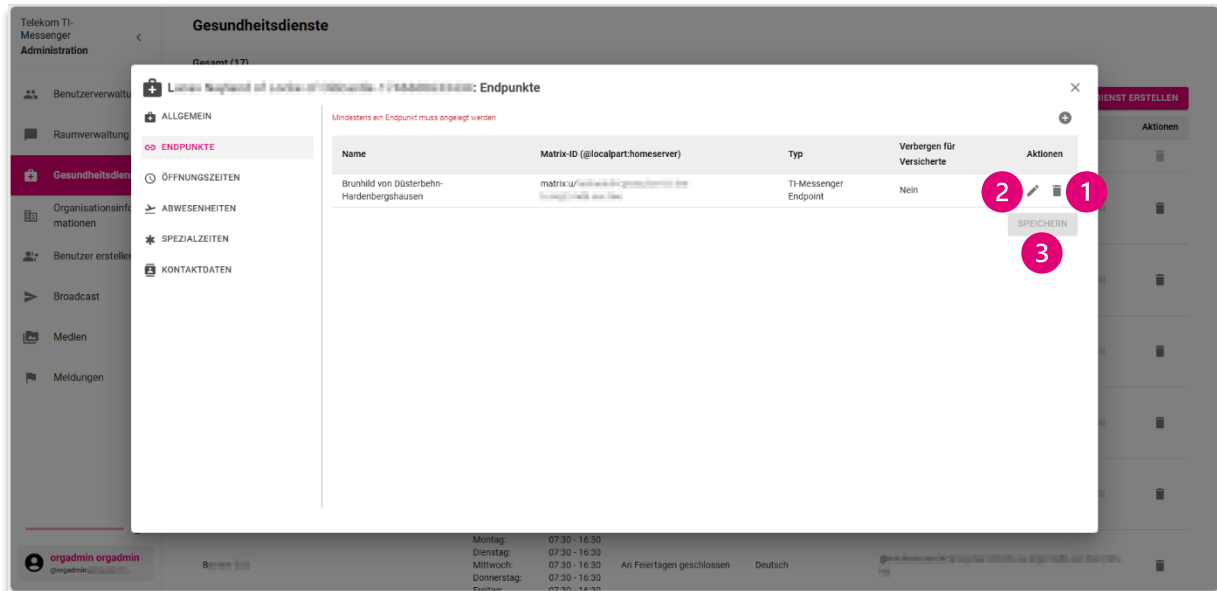
Im Reiter **[Allgemein]** können der Name und die Sprachen für Ihren Gesundheitsdienst festgelegt werden.



- 1 Im Feld **[Text]** können Sie einen Namen für den Gesundheitsdienst festlegen bzw. ändern.
- 2 Im Bereich Sprachen haben Sie die Möglichkeiten, Checkboxes für **Deutsch** und **Englisch** auszuwählen. Wählen Sie die Sprachen aus, in denen Ihr Gesundheitsdienst kommuniziert.
- 3 Falls Sie Änderungen vorgenommen haben, drücken Sie abschließend auf **[Speichern]**.

3.3.2 Endpunkte

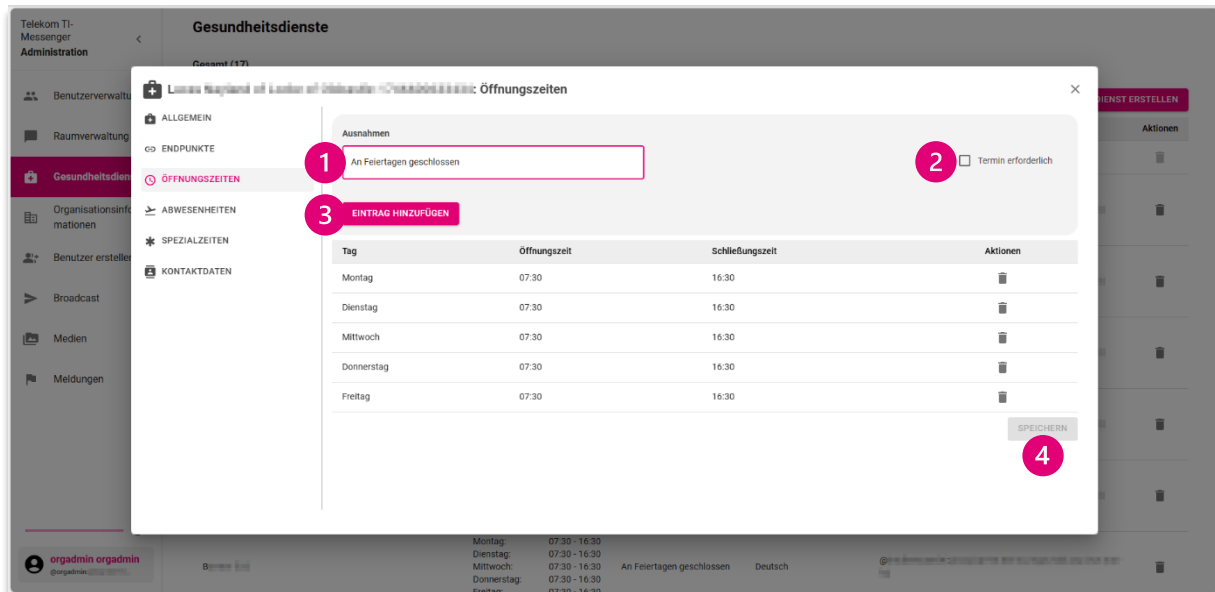
Im Reiter **[Endpunkte]** können Sie den Namen, die Matrix-ID, den Typ des Endpunktes und dessen Sichtbarkeit für Versicherte einsehen. Außerdem können Sie Endpunkte verwalten, indem Sie diese löschen.



- 1 In der Spalte **Aktionen** können Sie einen Endpunkt durch das Klicken auf das **Mülleimersymbol** löschen.
- 2 Wenn Sie den Endpunkt nachträglich bearbeiten wollen, klicken Sie auf das **Stift-Symbol**, links neben dem Mülleimer.
- 3 Falls Sie Änderungen vorgenommen haben, drücken Sie abschließend auf **[Speichern]**.

3.3.3 Öffnungszeiten

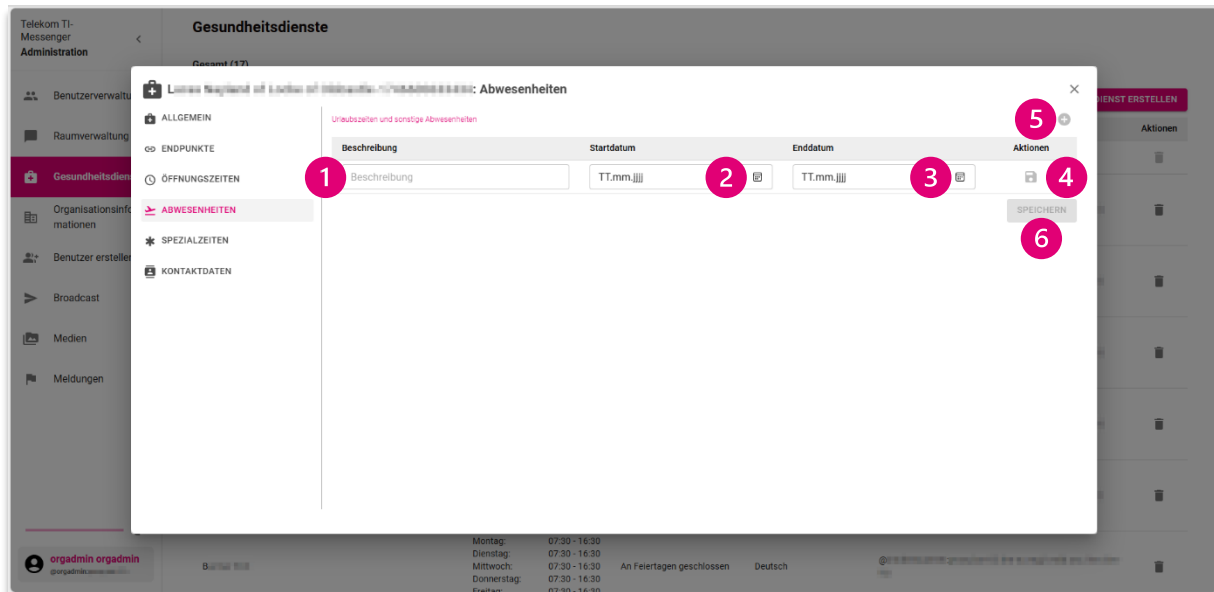
Im Reiter [Öffnungszeiten] können die Öffnungszeiten des Gesundheitsdienstes angepasst werden sowie Ausnahmen festgelegt werden.



- 1 Im Feld [Ausnahmen] können Ausnahmen für Öffnungszeiten des Gesundheitsdienstes im Freitext hinterlegt werden.
- 2 Wenn ein Termin für diesen Gesundheitsdienst erforderlich ist, können Sie dies über die **Checkbox** auswählen.
- 3 Wenn Sie einen Eintrag zu den Öffnungszeiten hinzufügen möchten, können Sie dies über den Button [Eintrag hinzufügen] machen.
- 4 Falls Sie Änderungen vorgenommen haben, drücken Sie abschließend auf [Speichern].

3.3.4 Abwesenheiten

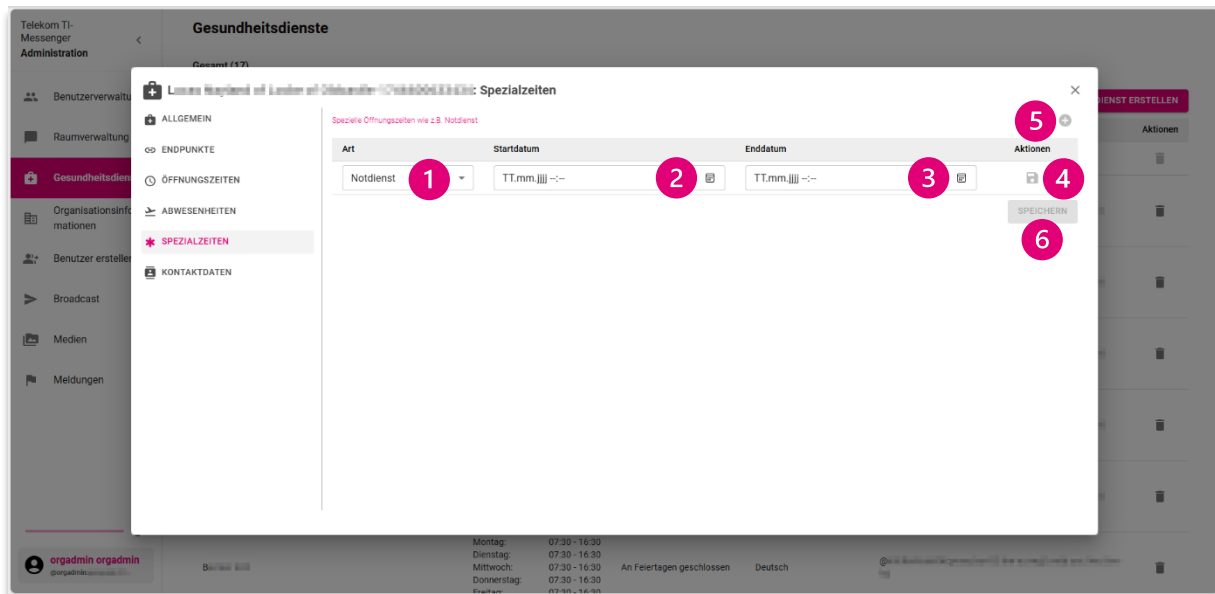
Im Reiter **[Abwesenheiten]** können Zeiten eingestellt werden, in denen der Gesundheitsdienst nicht erreichbar ist. Dabei kann eine Beschreibung sowie ein Start- und Enddatum festgelegt werden.



- 1 Im Feld **[Beschreibung]** können Sie eine Beschreibung für Ihre Abwesenheiten anlegen.
- 2 Hier müssen Sie ein **Startdatum** für Ihre Abwesenheit festlegen.
- 3 Hier müssen Sie ein **Enddatum** für Ihre Abwesenheit festlegen.
- 4 Wenn Sie eine Abwesenheit angelegt haben, klicken Sie auf das **Disketten-Symbol**.
- 5 Um eine weitere Abwesenheit hinzuzufügen, klicken Sie auf das **Plus-Symbol** und führen Schritte 1 bis 4 erneut mit Bezug auf die neue Abwesenheit aus.
- 6 Abschließend klicken Sie auf **[Speichern]**.

3.3.5 Spezialzeiten

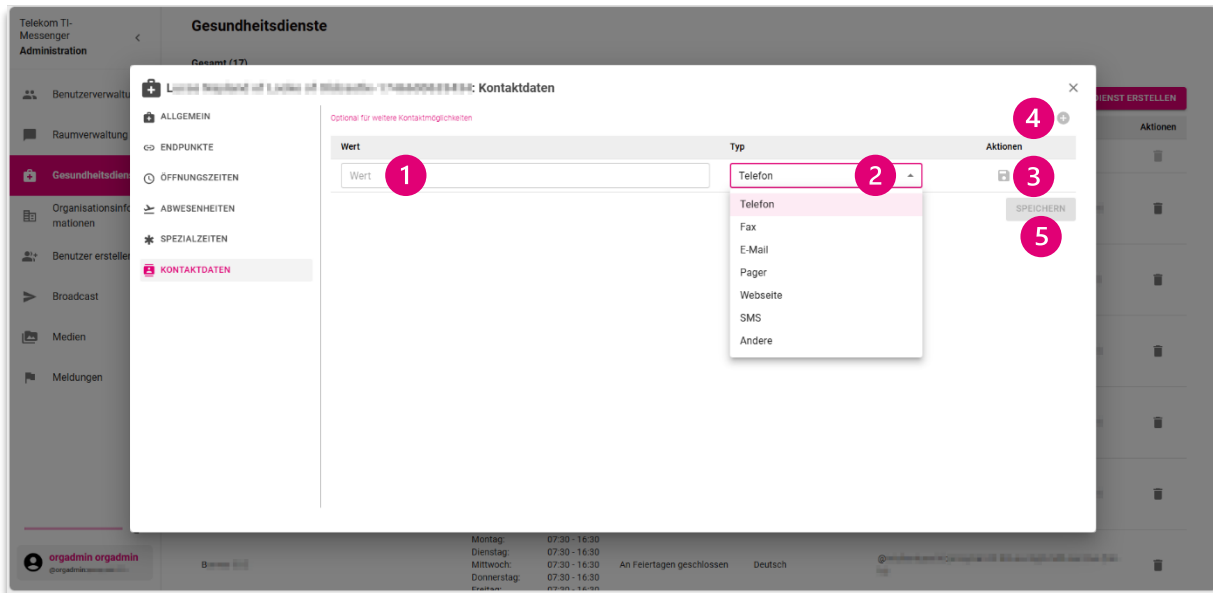
Im Reiter **[Spezialzeiten]** können Sie spezielle Öffnungszeiten wie z. B. Notdienste für den Gesundheitsdienst hinterlegen. Dabei kann eine Art, ein Start- und Enddatum festgelegt werden.



- 1 Im Feld **[Art]** können Sie in einem Menü den Grund der speziellen bzw. abweichenden Öffnungszeit auswählen.
- 2 Hier müssen Sie ein **Startdatum** für Ihre Spezialzeit festlegen.
- 3 Hier müssen Sie ein **Enddatum** für Ihre Spezialzeit festlegen.
- 4 Wenn Sie eine Spezialzeit angelegt haben, klicken Sie auf das **Disketten-Symbol**.
- 5 Um eine weitere Spezialzeit hinzuzufügen, klicken Sie auf das **Plus-Symbol** und führen Schritte 1 bis 4 erneut mit Bezug auf die neue Spezialzeit aus.
- 6 Abschließend klicken Sie auf **[Speichern]**.

3.3.6 Kontaktdaten

Im Reiter **[Kontaktdaten]** können optional weitere Kontaktmöglichkeiten für diesen Gesundheitsdienst hinterlegt werden.



- 1 Im Feld **[Wert]** können Sie die Daten entsprechend des gewählten Typs eingeben.
- 2 Im Feld **[Typ]** können Sie zwischen mehreren Optionen wählen, welche Art von Kontaktdaten Sie für Ihren Gesundheitsdienst hinterlegen möchten.
- 3 Wenn Sie Kontaktdaten angelegt haben, klicken Sie auf das **Disketten-Symbol**.
- 4 Um weitere Kontaktdaten hinzuzufügen, klicken Sie auf das **Plus-Symbol** und führen Schritte 1 bis 3 erneut mit Bezug auf die neuen Kontaktdaten aus.
- 5 Abschließend klicken Sie auf **[Speichern]**.

3.4 Gesundheitsdienst erstellen

In diesem Kapitel erfahren Sie, wie Sie einen neuen Gesundheitsdienst selbst anlegen können und was dabei zu beachten ist. Diese Funktion ermöglicht es Ihnen, Gesundheitsdienste für Benutzer zu erstellen, wodurch die Kommunikation und Informationsvermittlung schneller und effizienter gestaltet wird.

Name	Öffnungszeiten	Ausnahmen	Sprachen	Endpunkte	Aktionen
Organisationseintrag (@orgadmin:orgadmin@orgadmin.de)	Keine Öffnungszeiten angegeben	Keine Ausnahmen angegeben	Keine Sprachen angegeben	Keine Endpunkte angegeben	
Leistungsleistungen von... (@orgadmin:orgadmin@orgadmin.de)	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch	@orgadmin:orgadmin@orgadmin.de	
Fachbereich... (@orgadmin:orgadmin@orgadmin.de)	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch Englisch	@orgadmin:orgadmin@orgadmin.de	
Mittels... (@orgadmin:orgadmin@orgadmin.de)	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Englisch	@orgadmin:orgadmin@orgadmin.de	
Dienstleistungen... (@orgadmin:orgadmin@orgadmin.de)	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch	@orgadmin:orgadmin@orgadmin.de	
Kategorie... (@orgadmin:orgadmin@orgadmin.de)	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch Englisch	@orgadmin:orgadmin@orgadmin.de	
Bereich... (@orgadmin:orgadmin@orgadmin.de)	Montag: 07:30 - 16:30 Dienstag: 07:30 - 16:30 Mittwoch: 07:30 - 16:30 Donnerstag: 07:30 - 16:30 Freitag: 07:30 - 16:30	An Feiertagen geschlossen	Deutsch	@orgadmin:orgadmin@orgadmin.de	

1 Wenn Sie einen neuen Gesundheitsdienst anlegen wollen, klicken Sie auf den Button **[Gesundheitsdienste erstellen]**.

Die folgenden Unterkapitel bieten Ihnen eine detaillierte Anleitung zur Erstellung eines Gesundheitsdienstes.

3.4.1 Allgemeine Informationen

Beim Anlegen eines neuen Gesundheitsdienstes müssen Sie im ersten Schritt allgemeine Informationen eintragen.


The screenshot shows the 'Gesundheitsdienst erstellen' (Create Health Service) form in the Telekom TI-Messenger Administration interface. The form is divided into four steps: 1. Allgemeine Informationen, 2. Endpunkte, 3. Öffnungszeiten, and 4. Kontaktdaten Optional. The first step is active. It contains a 'Name' field with the value 'Test-Praxis' and a 'Sprachen' section with checkboxes for 'Deutsch' and 'Englisch', both of which are checked. There are 'ZURÜCKSETZEN', 'ZURÜCK', and 'WEITER' buttons. The left sidebar shows the 'Gesundheitsdienste' menu item highlighted. The user is logged in as 'orgadmin orgadmin'.

- 1 Geben Sie im Textfeld **[Name]** einen Namen für den Gesundheitsdienst an.
- 2 Wählen Sie dann aus, welche Sprachen in diesem Gesundheitsdienst gesprochen werden. Klicken Sie dafür die entsprechenden **Checkboxen** an.
- 3 Wenn Sie alles eingetragen haben, klicken Sie auf den Button **[Weiter]**.
- 4 Falls Sie zum vorhergehenden Reiter zurückkehren möchten, klicken Sie auf **[Zurück]**.

Anschließend werden Sie aufgefordert Endpunkte für Ihren Gesundheitsdienst einzugeben.

3.4.2 Endpunkte

Im nächsten Schritt müssen Sie mindestens einen Endpunkt eintragen, um den Dienst erstellen zu können.

Name	Matrix-ID (@localpart:homeserver)	Typ	Verbergen für Versicherte	Aktionen
Test_test	@hobias.prow.ti-messenger.org:org	TI-Messenger Endpoint	<input type="checkbox"/>	

Tragen Sie im Feld **Matrix-ID** die Matrix-ID des TI-Messenger-Profiles ein, über die der neue Gesundheitsdienst erreichbar sein soll.

Anschließend wählen Sie aus, um welchen **Typ** es sich bei dem Endpunkt handelt.

- 3 Falls der Endpunkt für die Versicherten verborgen werden soll, klicken Sie die **Checkbox** an.
- 4 Nach Eintragung aller Daten klicken Sie auf das **Disketten-Symbol**, um Ihre Daten abzuspeichern.
- 5 Wenn Sie alles eingetragen haben, klicken Sie auf den Button **[Weiter]**.
- 6 Sie können optional weitere Endpunkte für Ihren Gesundheitsdienst anlegen, indem Sie auf das **Plus-Symbol** klicken. Das Vorgehen bleibt für jeden weiteren Endpunkt das gleiche wie oben beschrieben.
- 7 Wenn Sie zum vorhergehenden Reiter zurückkehren möchten, klicken Sie auf den Button **[Zurück]**.

Anschließend werden Sie zum Anlegen der Öffnungszeiten weitergeleitet.

3.4.3 Öffnungszeiten

In diesem Kapitel erfahren Sie, wie Sie die Öffnungszeiten des Gesundheitsdienstes festlegen. Dadurch erhalten die Nutzer Informationen zur Erreichbarkeit des Dienstes.

Telekom TI-Messenger Administration

Gesundheitsdienst erstellen

1 Allgemeine Informationen 2 Endpunkte 3 Öffnungszeiten 4 Kontaktdaten Optional

Ausnahmen

1 An Feiertagen geschlossen

2 Termin erforderlich

3 EINTRAG HINZUFÜGEN

Weitere Zeiten wie z. B. Notdienstzeiten oder Urlaubszeiten können nach dem Erstellen angelegt werden.

Tag	Öffnungszeiten	Schließungszeit	Aktionen
Montag	07:30	16:30	
Dienstag	07:30	16:30	
Mittwoch	07:30	16:30	
Donnerstag	07:30	16:30	
Freitag	07:30	16:30	

ZURÜCKSETZEN

ZURÜCK WEITER

6 5

orgadmin orgadmin

- 1 Im Feld **Ausnahmen** können Sie für den Gesundheitsdienst im Freitext angeben, an welchen Tagen die regulären Öffnungszeiten nicht zutreffen (bspw. an Feiertagen).
- 2 Durch Anklicken der **Checkbox** können Sie festlegen, ob es für diesen Gesundheitsdienst erforderlich ist, einen Termin auszumachen.
- 3 Durch Klicken des Buttons **[Eintrag hinzufügen]** können Sie für einzelne Tage Ihre Öffnungszeiten hinzufügen.
- 4 Wenn die Öffnungszeiten für einen Wochentag geändert werden müssen, klicken sie auf das **Mülltonnen-Symbol** und löschen diesen Tag heraus. Anschließend fügen Sie durch Klicken des Buttons **[Eintrag hinzufügen]** für diesen Wochentag neue Öffnungszeiten hinzu.
- 5 Wenn Sie alles eingetragen haben, klicken Sie auf den Button **[Weiter]**.
- 6 Wenn Sie zum vorhergehenden Reiter zurückkehren möchten, klicken Sie auf den Button **[Zurück]**.

Anschließend werden Sie zum letzten Schritt weitergeleitet.

3.4.4 Kontaktdaten

Sie können in diesem Reiter optional Kontaktdaten für den Gesundheitsdienst hinterlegen, um so die Erreichbarkeit und Kommunikation zu stärken.

- 1 Falls Sie keine Kontaktdaten hinterlegen möchten, klicken Sie auf den Button **[Überspringen]**.
- 2 Falls Sie Kontaktdaten hinterlegen möchten, wählen Sie unter **Typ** die Art der Kontaktdaten aus.
- 3 Anschließend tragen Sie im Feld **[Wert]** die entsprechenden Kontaktdaten ein.
- 4 Um die Eingabe zu speichern, klicken Sie auf das **Disketten-Symbol**.
- 5 Wenn Sie alles eingetragen haben, klicken Sie auf den Button **[Weiter]**.
- 6 Zusätzlich können Sie weitere Kontaktdaten für Ihren Gesundheitsdienst hinterlegen. Klicken Sie dafür auf das **Plussymbol**, um eine weitere Kontaktmöglichkeit hinzuzufügen. Dieser Vorgang gestaltet sich für jede weitere Kontaktoption wie oben beschrieben.
- 7 Wenn Sie zum vorhergehenden Reiter zurückkehren möchten, klicken Sie auf den Button **[Zurück]**.

Abschließend werden Ihnen alle zuvor eingegebenen Daten in einer Übersicht angezeigt.

3.4.5 Zusammenfassung

Am Ende des Prozesses erhalten Sie abschließend die Möglichkeit alle zuvor eingegeben Daten des Gesundheitsdienstes zu überprüfen, bevor Sie ihn final anlegen.

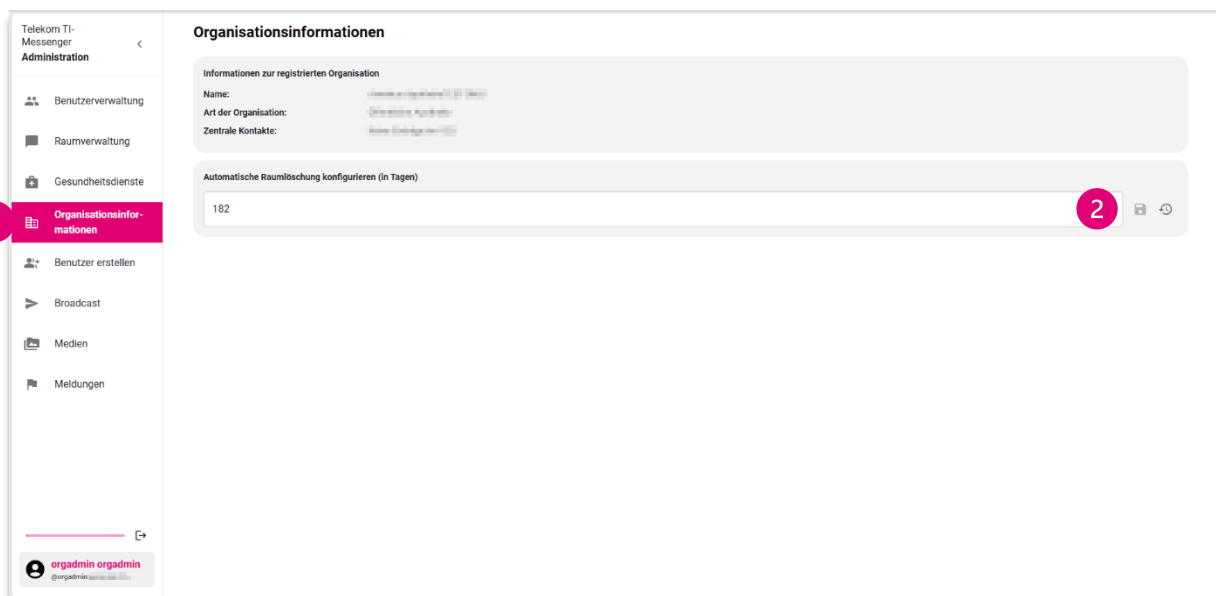
The screenshot shows the 'Gesundheitsdienst erstellen' (Create Health Service) form in the Telekom TI-Messenger Administration interface. The form is divided into four steps: 'Allgemeine Informationen', 'Endpunkte', 'Öffnungszeiten', and 'Kontaktdaten'. The 'Allgemeine Informationen' step is active, showing fields for Name, Endpunkte, Sprachen, Öffnungszeiten, and Kontaktdaten. A 'ZURÜCKSETZEN' button is located below the form, and 'ZURÜCK' and 'SPEICHERN' buttons are at the bottom right. Red circles with numbers 1, 2, and 3 highlight the 'SPEICHERN', 'ZURÜCKSETZEN', and 'SPEICHERN' buttons respectively.

- 1 Sollten Ihnen Unstimmigkeiten in Ihren Angaben aufgefallen sein, können Sie über den Button **[Zurück]** zum jeweiligen Reiter navigieren und die erforderlichen Korrekturen vornehmen.
- 2 Falls Sie sich entscheiden, den Gesundheitsdienst nicht zu erstellen, klicken Sie auf den Button **[Zurücksetzen]**.
- 3 Nachdem Sie alle eingegebenen Daten sorgfältig überprüft haben, klicken Sie abschließend auf **[Speichern]**. Sie haben erfolgreich einen neuen Gesundheitsdienst angelegt.

3.5 Organisationsinformationen

Im diesem Reiter erhalten Sie Informationen über Ihre Organisation, die von der gematik bereitgestellt werden. Diese Informationen werden automatisch abgerufen, nachdem Sie sich beim Registrierungsdienst authentifiziert haben.

Bitte beachten Sie, dass dieser Bereich lediglich zur Anzeige der Informationen dient. Änderungen an diesen Daten sind hier nicht möglich.

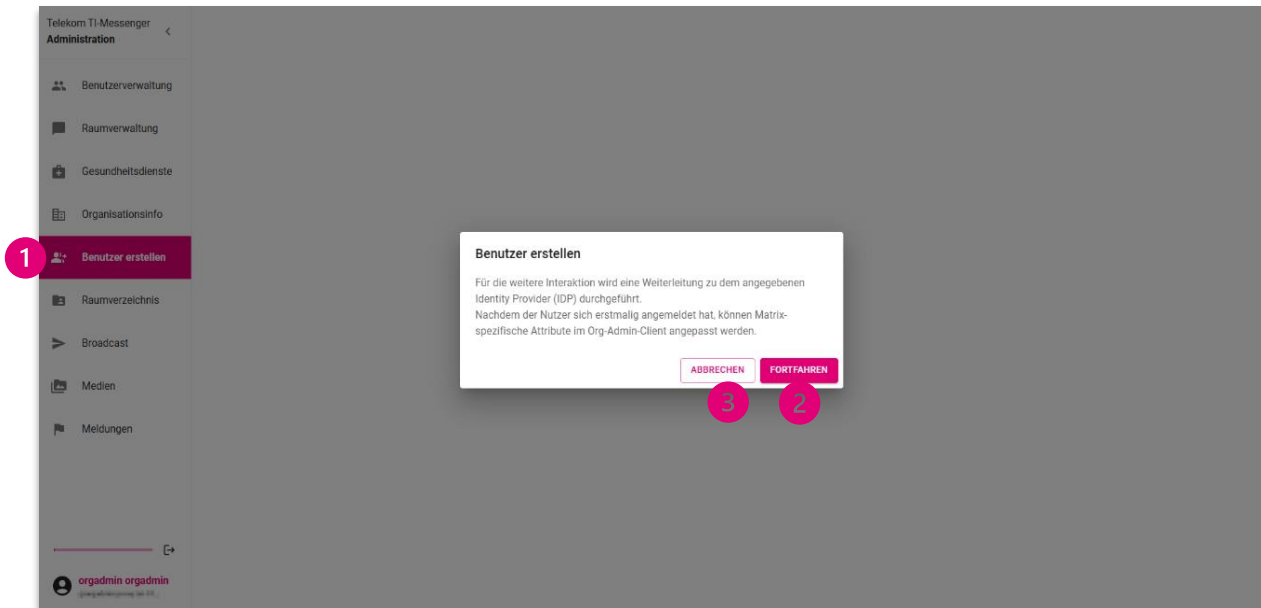


- 1 Unter **[Organisationsinfo]** können Sie die Informationen Ihrer registrierten Organisation von der gematik einsehen.
- 2 Um den Zeitraum, nach dem ein Raum im TI-Messenger Ihrer Organisation automatisch gelöscht wird, anzupassen, tragen Sie hier die gewünschte Anzahl von Tagen ein und klicken Sie auf das **Disketten-Symbol**, um die Angabe zu speichern. Standardmäßig erfolgt die automatische Raumlöschung nach einem halben Jahr.

3.6 Benutzer erstellen

In diesem Kapitel erfahren Sie, wie Sie neue Benutzer erstellen können. Es ist wichtig zu beachten, dass die Benutzer nicht direkt im Org-Admin angelegt werden. Um einen neuen Benutzer zu erstellen, klicken Sie auf den Reiter **[Benutzer erstellen]**. Ein Dialogfenster öffnet sich, in dem Sie darauf hingewiesen werden, dass Sie für alle weiteren Schritte zu dem angegebenen IDP weitergeleitet werden.

Bitte beachten Sie, dass Sie den Bereich des Org-Admin verlassen müssen, um die erforderlichen Schritte zur Benutzererstellung durchzuführen. Die genauen Anweisungen finden Sie in diesem Kapitel.

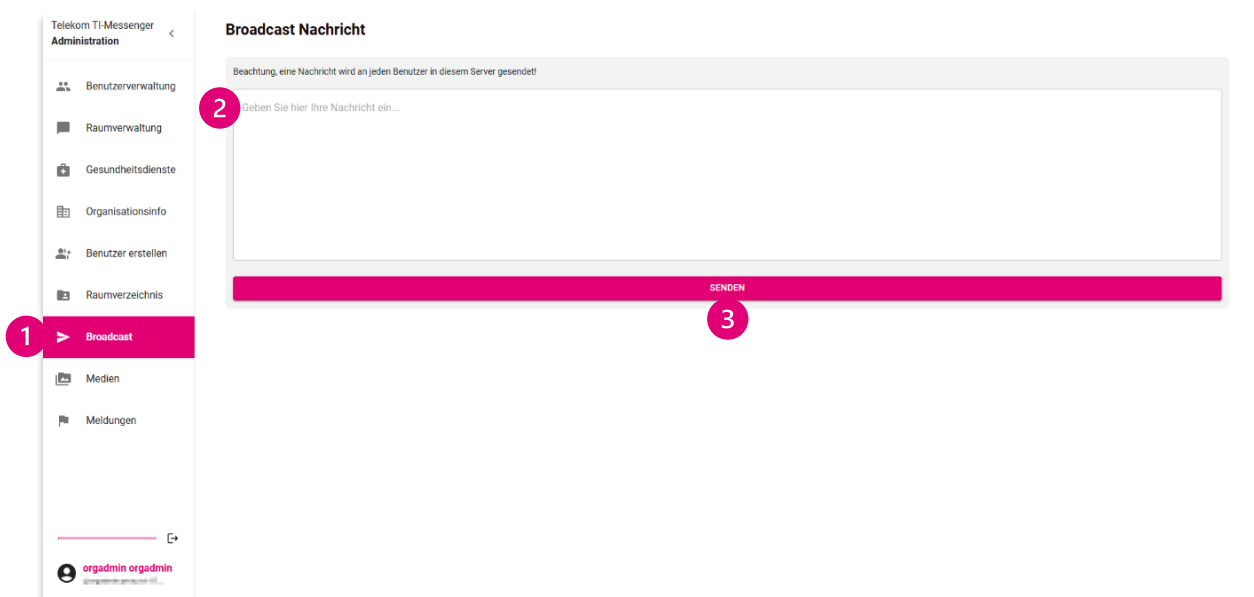


- 1 Unter **[Benutzer erstellen]** können Sie neue Nutzer anlegen.
- 2 Wenn Sie dies machen möchten, klicken Sie auf den Button **[Fortfahren]**. Der Button dient als **Absprung zu KeyCloak**. Mehr Informationen zu KeyCloak finden Sie in Kapitel 4.
- 3 Wenn Sie den Vorgang abbrechen möchten, klicken Sie auf **[Abbrechen]**.

3.7 Broadcast

In diesem Kapitel erfahren Sie, was Broadcast-Nachrichten sind und wie sie im TI-Messenger verwendet werden können. Broadcast-Nachrichten ermöglichen es Ihnen, wichtige Informationen schnell und effizient an eine Vielzahl von Empfängern zu übermitteln, ohne dass individuelle Nachrichten verfasst und gesendet werden müssen.

Durch die Nutzung von Broadcast-Nachrichten können Administratoren und Benutzer sicherstellen, dass alle Mitglieder eines Raums zur gleichen Zeit über relevante Updates, Ankündigungen oder wichtige Informationen informiert werden. Diese Funktion verbessert die Kommunikationsstruktur und erhöht die Reaktionsfähigkeit innerhalb Ihrer Organisation, indem sie eine konsistente und koordinierte Informationsverteilung gewährleistet.



- 1 Unter **[Broadcast]** haben Sie die Möglichkeit, eine Nachricht an alle Nutzer auf Ihrem Homeserver zu senden.
- 2 Um eine Broadcast-Nachricht zu versenden, verfassen Sie eine Nachricht im Feld **[Geben Sie hier Ihre Nachricht ein...]**.
- 3 Klicken Sie anschließend auf **[Senden]**. Beachten Sie, dass die Nachricht direkt gesendet wird und keine zusätzliche Abfrage stattfindet. Die Nachricht wird bei den Benutzern im Raum „Server Notices“ angezeigt.

3.8 Medien

In diesem Kapitel erhalten Sie umfassende Informationen zu den Medien, die von Nutzern auf Ihrem Homeserver versendet wurden. Sie erfahren, wie Sie die Medien nach Benutzer-ID, Anzeigename, Medienanzahl und Mediengröße einsehen können. Zudem haben Sie die Möglichkeit, im Falle von Sicherheitsvorfällen verdächtige Medien unter „Quarantäne“ zu setzen, um die Sicherheit Ihrer Umgebung zu gewährleisten.

Benutzer-ID	Anzeigename	Medienanzahl	Mediengröße	Aktionen
@[User-ID]:[Homeserver]	[Anzeigename]	2	0.34	[Aktionen]
@orgadmin:[Homeserver]	orgadmin orgadmin	4	0.19	[Aktionen]
@[User-ID]:[Homeserver]	[Anzeigename]	2	0.1	[Aktionen]

1 Die Übersicht bietet Ihnen wichtige Informationen zu den Medien eines Nutzers und ist folgendermaßen strukturiert:

- **Benutzer-ID:** Endpunkt des Nutzers im Format @[User-ID]:[Homeserver];
- **Anzeigename:** Der aktuelle Anzeigename des Nutzers;
- **Medienanzahl:** Die Anzahl der vom Nutzer versandten Medien;
- **Mediengröße:** Die gesamte Dateigröße aller versandten Medien des Nutzer in GB;
- **Aktionen:** Möglichkeit, alle Dateien des Nutzers unter Quarantäne zu setzen. 🚫

Hinweis: Bitte beachten Sie, dass diese Aktion im TI-Messenger nicht anwendbar ist, da es sich um verschlüsselte Chats handelt, auf die der Org-Admin keinen Zugriff hat.

2 Die Liste ist standardmäßig nach absteigender Mediengröße sortiert, erkennbar an dem Pfeilsymbol. Mit einem **Klick** auf eine der grauhinterlegten **Spaltenüberschriften** sortieren Sie die Liste alpha-numerisch absteigend nach der entsprechenden Spalte. Mit einem zweiten Klick auf die jeweilige Spaltenüberschrift kehren Sie die Sortierung um.

3 Zusätzlich können Sie über die Funktion **[Exportieren (CSV)]** eine vollständige Liste der Medien im CSV-Dateiformat herunterladen.

- 4 Durch einen Klick auf eine einzelne **Zeile** in der Liste erhalten Sie Detailinformationen zu den hochgeladenen Medien eines spezifischen Nutzers. Wie diese aussieht und welche Informationen Sie dort einsehen können, wird nachfolgend beschrieben.

In diesem Abschnitt wird Ihnen eine Übersicht über alle Medien angezeigt, die einem bestimmten Nutzer zugeordnet sind. Diese klare Zuordnung ermöglicht es Ihnen, gezielt auf bestimmte Medien zu reagieren, insbesondere im Falle von Sicherheitsvorfällen.


Dateiname	Letzter Zugriff	Medien-ID	Medientyp	Erstellt am ↓	Unter Quarantäne gestellt von	Aktionen
Nicht verfügbar	22.1.2026, 15:41:11	XXXXXXXXXXXXXXXXXXXX	application/octet-stream	22.1.2026, 15:40:46	Niemand	1 2 3 4
Nicht verfügbar	Nie	XXXXXXXXXXXXXXXXXXXX	application/octet-stream	22.1.2026, 15:40:46	Niemand	1 2 3 4
Nicht verfügbar	22.1.2026, 15:41:11	XXXXXXXXXXXXXXXXXXXX	application/octet-stream	22.1.2026, 15:40:38	Niemand	1 2 3 4
Nicht verfügbar	Nie	XXXXXXXXXXXXXXXXXXXX	application/octet-stream	22.1.2026, 15:40:38	Niemand	1 2 3 4

Die Liste zu den individuellen Medien der Nutzer enthält folgende Informationen:

- **Dateiname:** Der Name der Datei;
- **Letzter Zugriff:** Datum und Uhrzeit des letzten Zugriffs auf die Datei, z. B. beim Anzeigen von Bildern oder Herunterladen von Dokumenten (ggf. „Nie“);
- **Medien-ID:** Eine 24-stellige Kombination aus Klein- und Großbuchstaben, die eindeutig ein Medium zuordnet;
- **Medientyp:** Der Dateityp und das Format des einzelnen Mediums;
- **Erstellt am:** Das ursprüngliche Hochlade- oder Versanddatum des Mediums;
- **Unter Quarantäne gestellt von:** Endpunkt des Nutzers in der Rolle des Org-Admins, der das Medium unter Quarantäne gestellt hat;
- **Aktionen:** Sie haben die folgenden Handlungsmöglichkeiten:

- 1 **Datei herunterladen** (im angegebenen Dateiformat).
- 2 **Schützen** Eine geschützte Datei kann von einem anderen User in der Rolle Org-Admin nicht mehr unter Quarantäne gestellt werden.
- 3 **Unter Quarantäne stellen** Der Zugriff auf die Datei wird gesperrt.

4

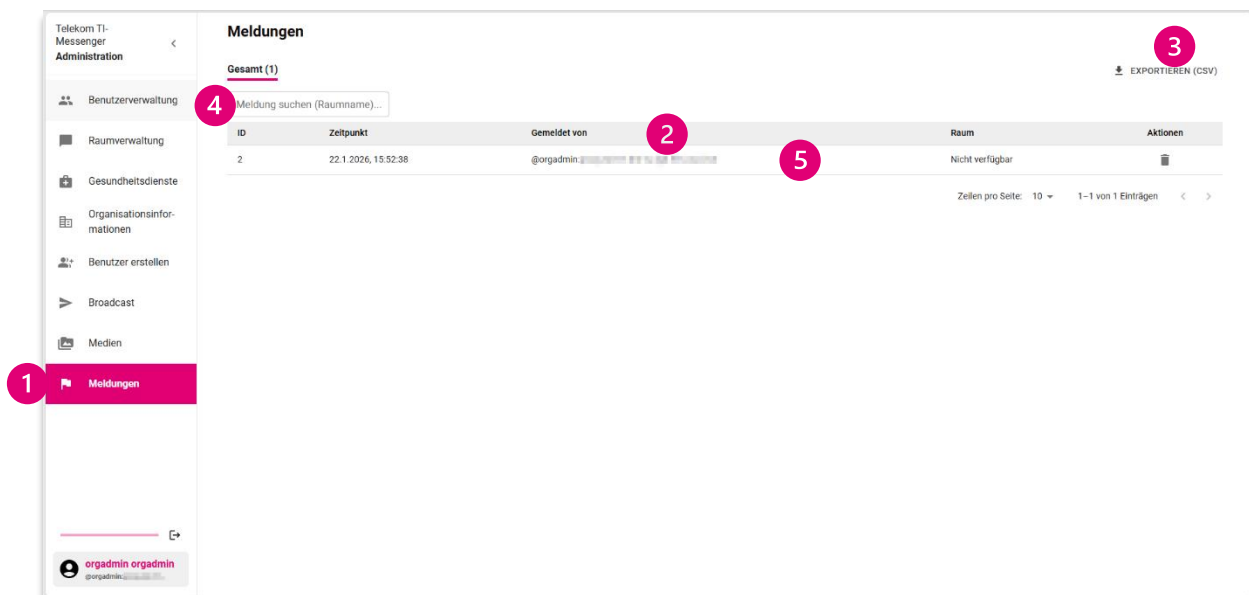
Datei löschen  Diese Aktion ist im TI-Messenger nicht anwendbar, da es sich um verschlüsselte Chats handelt und der Org-Admin darauf keinen Zugriff hat.

Hinweis: Bitte beachten Sie, dass die Aktion „Unter Quarantäne stellen“ im TI-Messenger nicht anwendbar ist, da es sich um verschlüsselte Chats handelt, auf die der Org-Admin keinen Zugriff hat.

3.9 Meldungen

In diesem Kapitel erfahren Sie die Bedeutung einer Meldung und wie Sie mit diesen umgehen können. Meldungen werden von Mitgliedern eines Chats abgegeben, wenn Sie eine Nachricht als unangemessen empfinden. Sie erfahren, wie Meldungen strukturiert sind und wie man auf die verschiedenen Informationen zugreifen kann, um einen umfassenden Überblick über die gemeldeten Inhalte zu erhalten.

Durch das Klicken auf eine einzelne Meldung können Sie detaillierte Informationen einsehen, einschließlich Zeitstempel, den verantwortlichen Benutzer und den spezifischen Grund der Meldung. Dies hilft Ihnen, potenzielle Probleme schnell zu identifizieren und fundierte Entscheidungen zu treffen, um ein sicheres und respektvolles Kommunikationsumfeld aufrechtzuerhalten.



1 Im Reiter **[Meldungen]** erhalten Sie eine Liste der Meldungen aus allen Chaträumen auf dem von Ihnen verwalteten Homeserver. Die Liste enthält folgende Informationen:

- **ID:** Eindeutige fortlaufende Identifikationsnummer einer einzelnen Meldung;
- **Zeitpunkt:** Datum und Uhrzeit der Meldung;
- **Gemeldet von:** Endpunkt des Nutzers in der Form @[Username]:[Homeserver], der die entsprechende Meldung ausgelöst hat;
- **Raum:** Name des Raumes, in dem die gemeldete Nachricht geschickt wurde;
- **Aktionen:** Möglichkeit zum Löschen einer Meldung durch Klicken auf das Mülleimersymbol.

2 Die Liste ist standardmäßig alphabetisch absteigend nach Meldungs-ID sortiert, erkennbar an dem Pfeilsymbol. Mit einem **Klick** auf eine der grauhinterlegten **Spaltenüberschriften** sortieren Sie die Liste alpha-numerisch absteigend nach der entsprechenden Spalte. Mit einem zweiten Klick auf die jeweilige Spaltenüberschrift kehren Sie die Sortierung um.

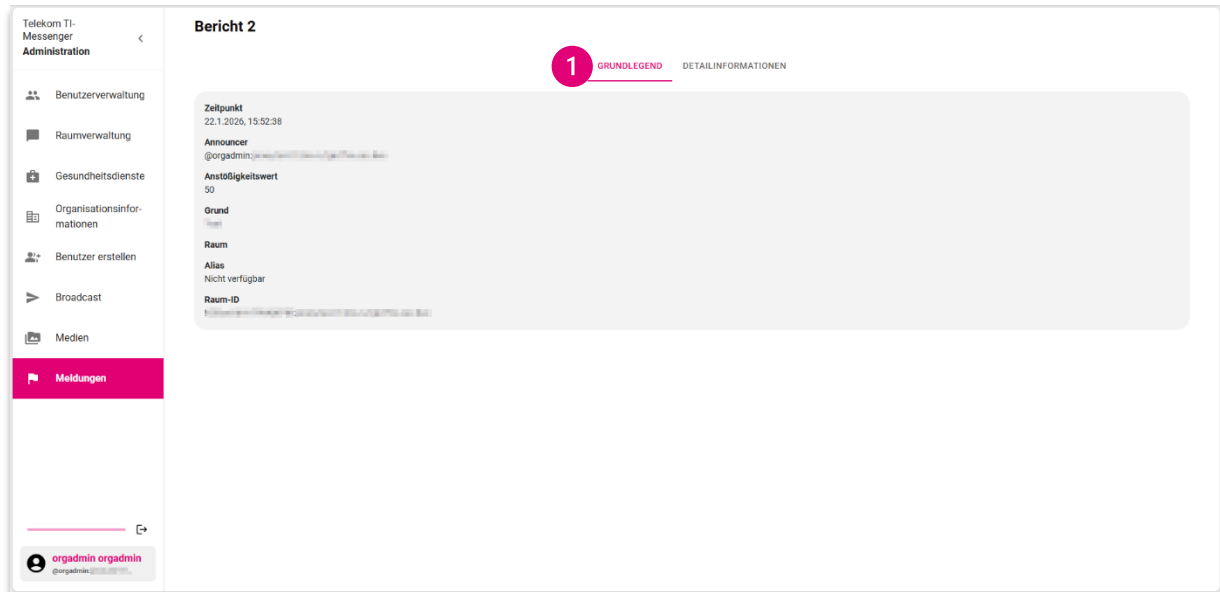
3 Darüber hinaus können Sie über die Funktion **[Exportieren (CSV)]** eine vollständige Liste der Meldungen im CSV-Dateiformat herunterladen.

4 Im Feld **[Meldung suchen (Raumname)...]** können sie nach spezifischen Meldungen anhand des Raumnamens suchen.

5 Klicken Sie auf die Zeile einer **Meldung**, um Detailinformationen zu den Meldungen einzusehen.

3.9.1 Grundlegend

In diesem Kapitel erhalten Sie grundlegende Informationen zu den Meldungen aus den jeweiligen Chats. Hierbei ist vor allem der Grund der Meldung wichtig, um einschätzen zu können, warum die Nachricht gemeldet wurde.



1 Klicken Sie auf eine einzelne Meldung, können Sie unter **[Grundlegend]** weitere Informationen einsehen:

- **Zeitpunkt:** Datum und Uhrzeit der Meldung;
- **Announcer:** Endpunkt des meldenden Nutzers in der Form @[Username]:[Homeserver];
- **Anstößigkeitswert:** Score zwischen 0 und 100, der die Schwere der Anstößigkeit einer Nachricht einstuft (z. B. Regelverstoß < Beleidigung < Morddrohung);
- **Grund:** Grund, warum die Nachricht gemeldet wurde. In diesem Feld steht nur dann etwas, wenn der meldende User auch einen Grund zur Meldung angegeben hat. Ansonsten ist das Feld leer;
- **Raum:** Titel des Raumes, in dem die gemeldete Nachricht versandt wurde;
- **Alias:** Alternativer Raumname, z. B. #support:homeserver.de;
- **Raum-ID:** Eindeutige fortlaufende Identifikationsnummer einzelner Räume.

4 Absprung: KeyCloak

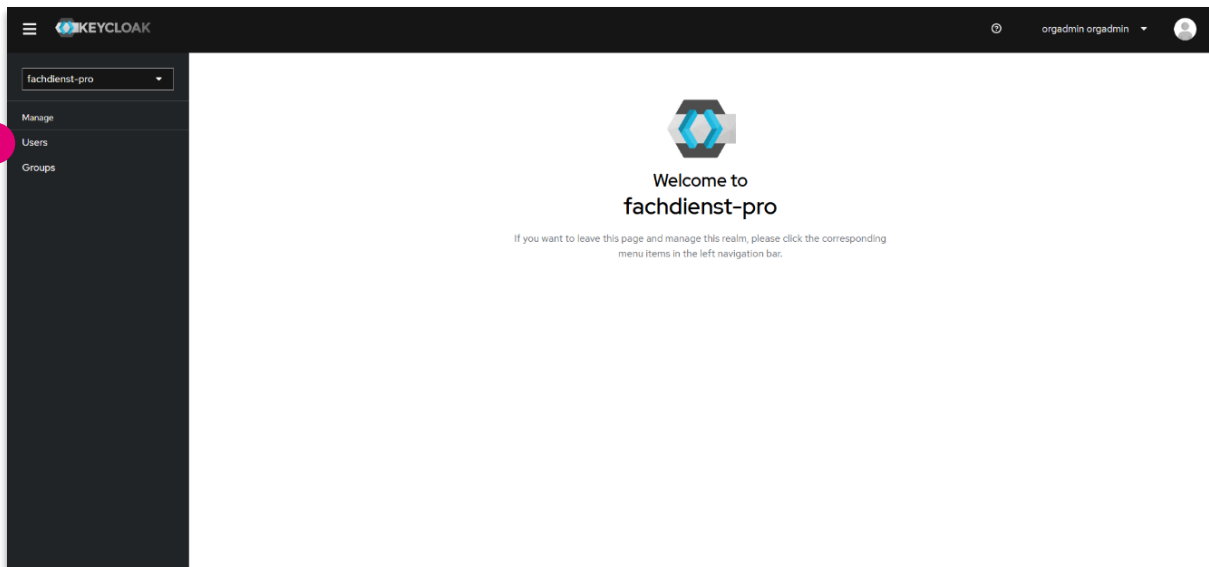
KeyCloak ist ein Open-Source-Tool, welches dabei hilft, Benutzeranmeldung und -verwaltung in Anwendungen einfacher und sicherer zu machen. Es übernimmt Aufgaben wie Login, Logout und Passwortverwaltung. Statt diese Funktionen selbst zu programmieren, kann man sie mit KeyCloak zentral verwalten. Nützlich ist KeyCloak in größeren Systemen mit mehreren Anwendungen, weil Benutzer sich nur einmal anmelden müssen, um alle Dienste nutzen zu können (Single Sign-On).

Wenn Sie den Absprungpunkt **[Fortfahren]** in Kapitel 3.6 ausgewählt haben, gelangen Sie zum KeyCloak für den Fachdienst Pro. Es kann sein, dass Sie erneut Ihre Nutzerdaten eingeben müssen. Nehmen Sie die gleichen Nutzerdaten, die Sie zur Anmeldung des Org-Admins verwendet haben.

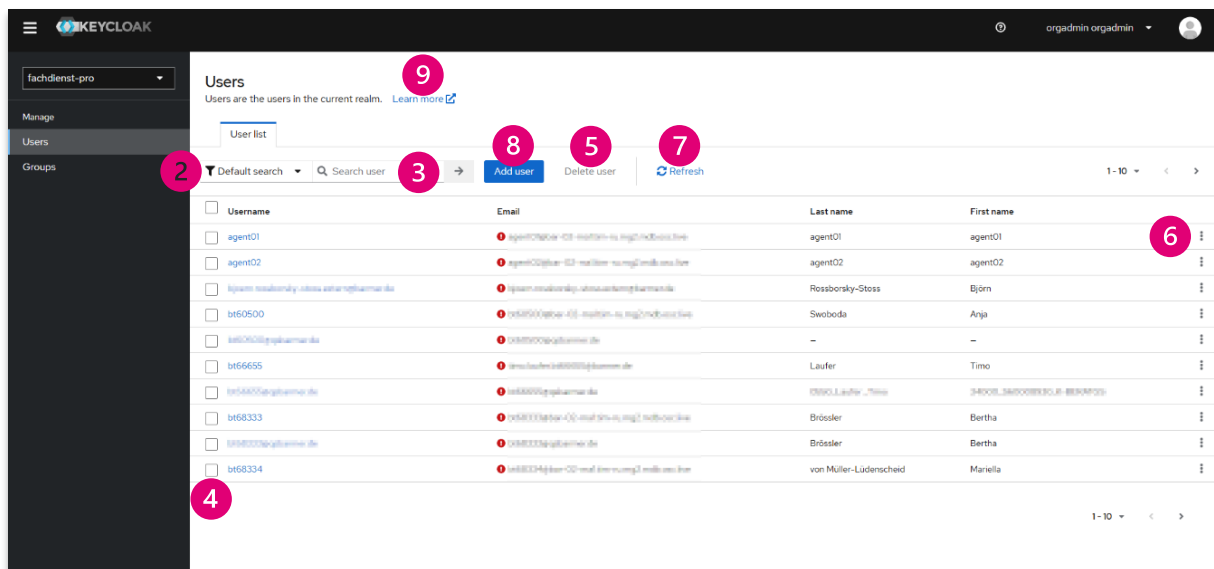
Durch den Absprungpunkt gelangen Sie auf die Benutzeroberfläche des KeyCloak des Fachdienst Pro. Die standardmäßige Spracheinstellung ist Englisch.

4.1 KeyCloak: Users

Im Reiter Users haben Sie die Möglichkeit, dezidiert die User zu managen. Dazu zählt, dass Sie neue User anlegen können, die Eigenschaften und Rechte eines Users einstellen können und die Default Einstellungen einsehen können.



1 Klicken Sie auf den Reiter **[Users]**, um weitere Optionen angezeigt zu bekommen.



- 2 Sie haben durch Klicken auf das Feld **[Default search]** die Möglichkeit, Ihre Suche zu verändern. Wenn hier die Option **[Default search]** ausgewählt ist, können Sie nach den Namen von Nutzern suchen. Durch Klicken auf das Feld **[Default search]** öffnet sich die Option **[Attribute search]**. Wenn Attribute Search ausgewählt ist, können Sie nach bestimmten Attributen von Usern suchen.
- 3 Im Feld **[Search user]** können Sie durch Freitexteingabe entsprechend Ihrer obigen Auswahl nach bestimmten Usern oder Attributen suchen.
- 4 Links neben den Usernamen befinden sich Checkboxes. Sie können durch Anklicken der **Checkboxes** einen oder mehrere User auswählen. Wenn Sie die Checkbox neben dem Spaltentitel „Username“ anklicken, wählen Sie automatisch alle User aus der Liste aus.
- 5 Sie haben die Möglichkeit, die zuvor ausgewählten User durch Klicken auf den Button **[Delete user]** zu löschen.
- 6 Alternativ befindet sich rechts neben der Spalte „First name“ in jeder Zeile ein **Drei-Punkte-Menü**. Wenn Sie daraufklicken, haben Sie ebenfalls die Möglichkeit, den bzw. die ausgewählten User zu löschen.
- 7 Wenn Sie auf den Button **[Refresh]** anklicken, können Sie die Seite aktualisieren.
- 8 Um einen weiteren User anzulegen, klicken Sie auf den Button **[Add user]**. Es öffnet sich ein weiteres Fenster, in welchem Sie den User anlegen können. Mehr Informationen dazu finden Sie in Kapitel 4.2.
- 9 Wenn Sie mehr zum System und dessen Optionen erfahren möchten, klicken Sie auf den Absprungpunkt **[Learn more]**.

4.2 KeyCloak: Neue User anlegen

Wie in Kapitel 4.1 erwähnt, gelangen Sie durch Klicken auf den Button **[Add user]** zu einer Eingabemaske, um einen neuen User anzulegen. Im Folgenden wird beschrieben, wie Sie diese korrekt befüllen.

The screenshot shows the Keycloak 'Create user' interface. The form is titled 'Create user' and is part of the 'Users' management section. It features a sidebar with navigation options like 'Manage', 'Users', and 'Groups'. The main form area includes a 'Required user actions' dropdown menu (1), an 'Email verified' toggle switch (2), and a 'General' section with input fields for 'email' (3), 'username' (4), 'firstName' (5), and 'lastName' (6). There is also a 'Chatbot' dropdown menu (7) and a 'Groups' section with a 'Join Groups' button (8). At the bottom, there are 'Create' (9) and 'Cancel' (10) buttons. A 'Jump to section' dropdown is also visible, currently set to 'General'.

1 Durch Klicken auf das Feld **[Select action]**, legen Sie fest welche Aktion vom User gefordert wird. Wählen Sie die passende Option:

- **Configure OTP:** Erfordert die Einrichtung eines mobilen Passwortgenerators;
- **Update Password:** Erfordert die Eingabe eines neuen Passworts;
- **Update Profile:** Erfordert die Eingabe neuer persönlicher Daten;
- **Verify Email:** Sendet dem Benutzer eine E-Mail, um seine E-Mail-Adresse zu bestätigen;
- **Webauthn Register:** Alternativen für die 2FA, um diese neu oder initial einzurichten;
- **Verify Profile:** Verifizieren Sie Ihr Profil.

Die folgenden Optionen erfüllen im TI-Messenger keinen Zweck:

- Webauthn Register Passwordless;
- Update User Locale.

2 Mit dem **Schieberegler** können Sie angeben, ob die E-Mail-Adresse dieses Users bereits verifiziert wurde oder nicht. Stellen Sie den Schieberegler entsprechend ein.

3 Im Feld **email** geben Sie die E-Mail-Adresse des Users ein.

4 Im Feld **username** geben Sie den Usernamen des Users ein.

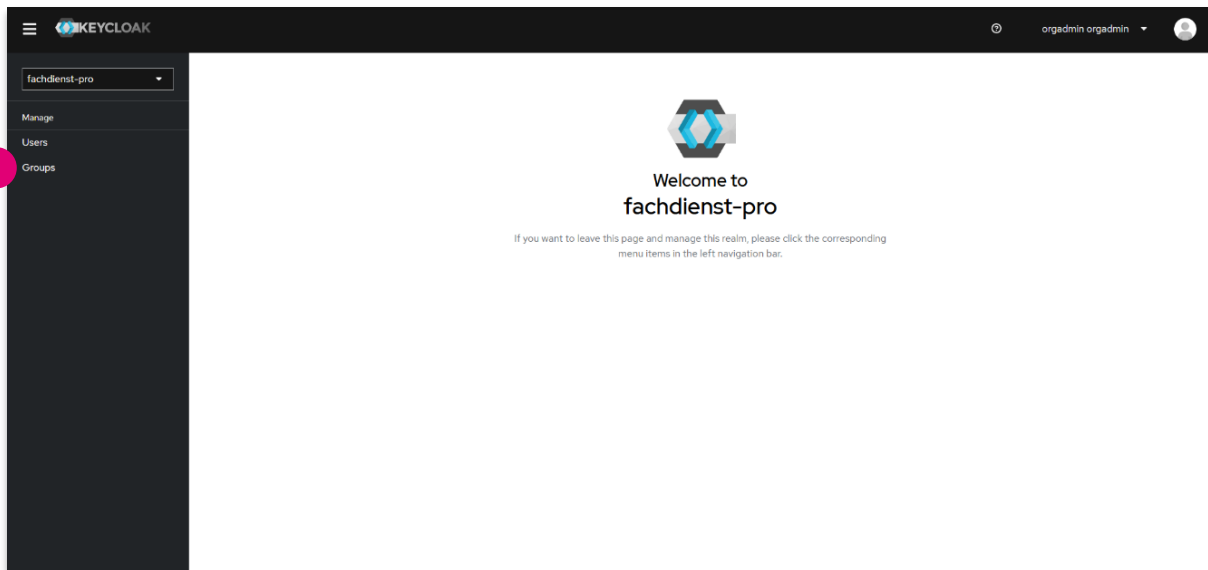
5 Im Feld **firstName** geben Sie den Vornamen des Users ein.

6 Im Feld **lastName** geben Sie den Nachnamen des Users ein.

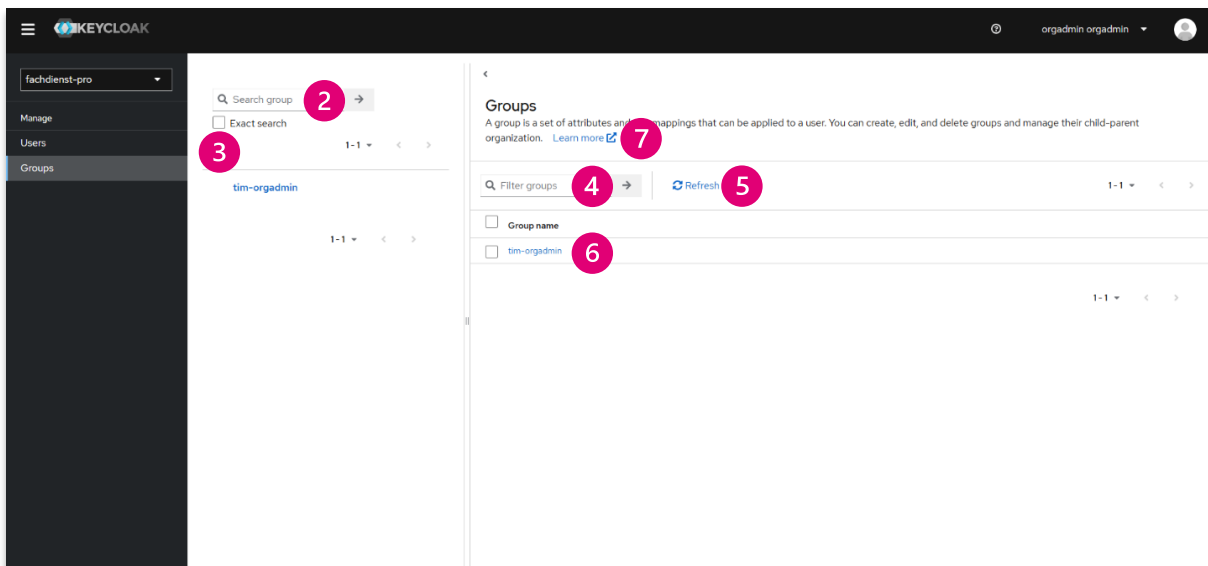
7 Im Feld **Chatbot** können Sie auswählen, ob der von Ihnen angelegte User ein Chatbot ist oder nicht.

- 8 Durch Klicken auf den Button **[Join Groups]** können Sie den User in Gruppen hinzufügen.
- 9 Nach der Eingabe aller Daten klicken Sie abschließend auf den Button **[Create]**, um den User final anzulegen.
- 10 Wenn Sie den Vorgang abbrechen möchten, klicken Sie auf den Button **[Cancel]**.

4.3 KeyCloak: Groups



- 1 Klicken Sie auf den Reiter **[Groups]**, um weitere Optionen angezeigt zu bekommen.

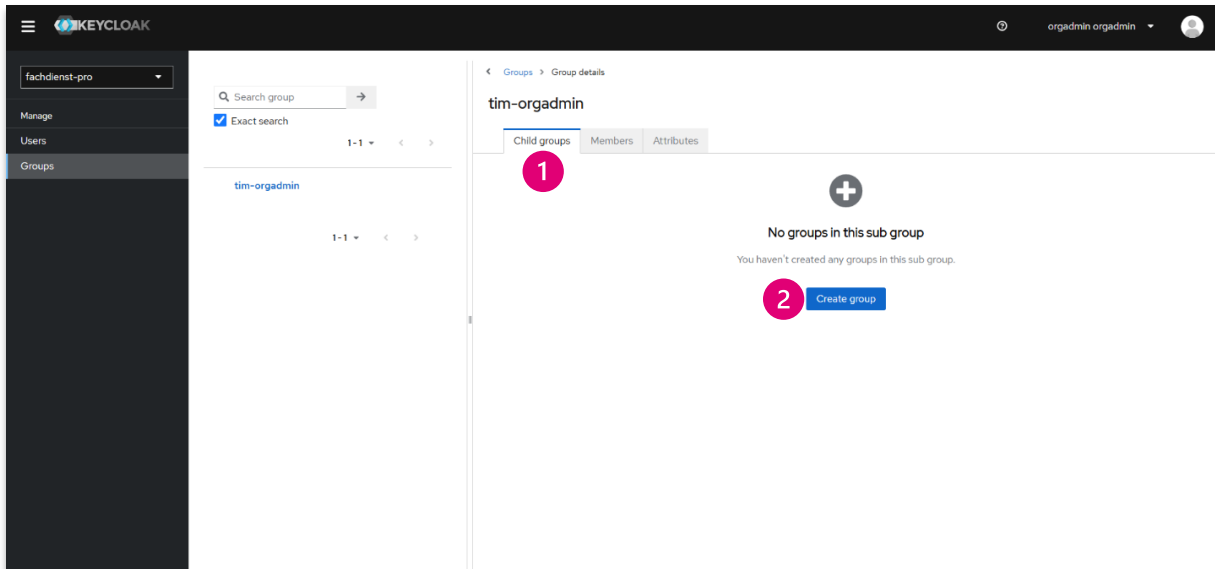


- 2 Wenn Sie in das Feld **[Search group]** klicken, können Sie gezielt nach Gruppen suchen.
- 3 Durch das Anklicken der Checkbox **[Exact search]** werden Ihnen nur die Suchergebnisse geliefert, die exakt mit der Zeichenfolge Ihrer Suchanfrage übereinstimmen. Wenn Sie also bspw. nach Teilwörtern suchen wollen, eignet sich diese Sucheinstellung nicht.
- 4 Das Feld **[Filter groups]** ermöglicht es Ihnen, bei den bestehenden Gruppen nach bestimmten Merkmalen zu filtern, um Ihre Suche weiter einzugrenzen.
- 5 Wenn Sie die Ergebnisse bzw. Ihre Ansicht aktualisieren möchten, klicken Sie auf den Button **[Refresh]**.
- 6 Wenn Sie eine bestimmte Gruppe auswählen möchten, **klicken** Sie auf die Gruppe.

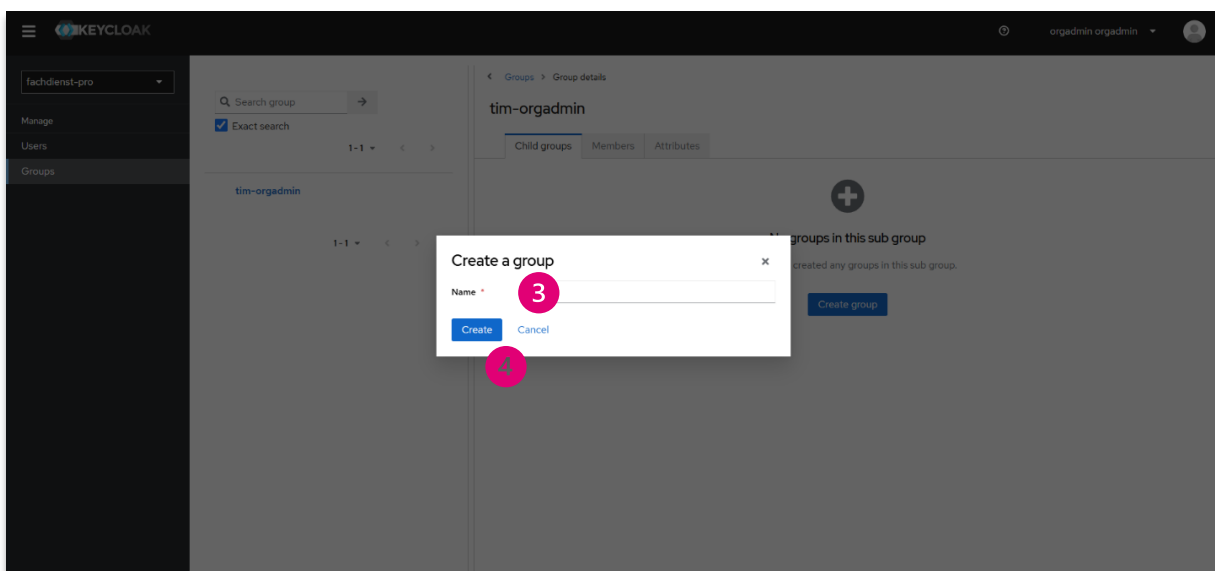
- 7 Um mehr über Gruppen und deren Einstellungen zu erfahren, klicken Sie auf den Absprung **[Learn more]**.

4.4 KeyCloak: Ausgewählte Gruppe

Wenn Sie in Kapitel 4.3 Schritt 6 durchgeführt haben, befinden Sie sich in der Bearbeitungsansicht für die zuvor ausgewählte Gruppe.

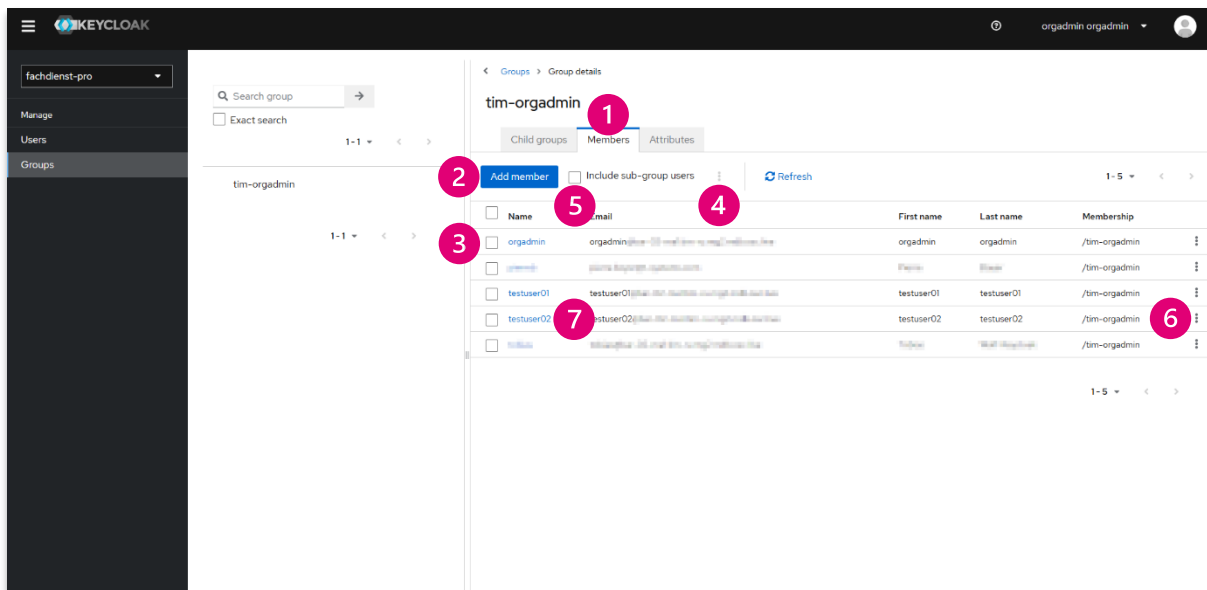


- 1 Im ersten Reiter „**Child groups**“ können Sie einsehen, ob zu der von Ihnen ausgewählten Gruppe noch weitere Subgruppen existieren.
- 2 Sie können selbst eine neue Subgruppe anlegen, indem Sie auf den Button **[Create group]** klicken.



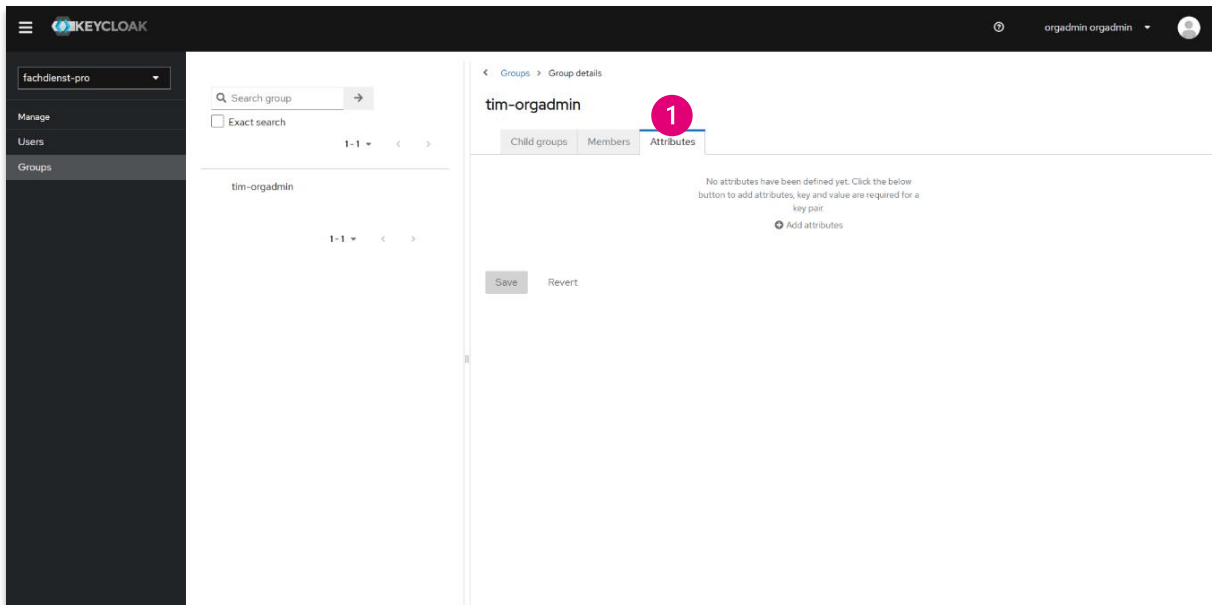
- 3 Es öffnet sich ein Fenster, in welchem Sie der Subgruppe einen **Namen** geben müssen.
- 4 Klicken Sie abschließend auf den Button **[Create]**, um die Subgruppe zu erstellen. Falls Sie den Vorgang abbrechen möchten, klicken Sie auf den Button **[Cancel]**.

Der Bereich „**Members**“ zeigt, welche Mitglieder sich in der Gruppe befinden. Sie erhalten hier die Möglichkeit die Gruppe zu managen und aktuell zu halten.



- 1 Klicken Sie auf den Reiter **[Members]**, um die einzelnen Mitglieder der aufgerufenen Gruppe anzuzeigen. Sie erhalten eine alphabetische Auflistung aller bestehenden Gruppenmitglieder mit deren Name, E-Mail-Adresse, Vor- und Nachname und deren Mitgliedschaft in der Gruppe.
- 2 Sie können durch klicken auf den Button **[Add member]** weitere Mitglieder in diese Gruppe hinzufügen.
- 3 Links neben jedem User befindet sich eine **Checkbox**, welche Sie anklicken können. (Durch Auswahl eines oder mehrerer User können Sie die ausgewählten User, wie in Schritt 4 beschrieben, entfernen.)
- 4 Über das **Drei-Punkte-Menü** können Sie die in Schritt 3 ausgewählten User aus der Gruppe entfernen.
- 5 Durch Anklicken der **Checkbox** werden auch die Mitglieder in der Anzeige dargestellt, die sich in Subgruppen befinden.
- 6 Wenn Sie einzelne User aus der Gruppe entfernen wollen, befindet sich am Ende jeder Zeile das **Drei-Punkte Menü**. Klicken Sie dieses an, eröffnet sich die Option den User aus der Gruppe zu entfernen. Sollten Sie sich anders entscheiden klicken Sie neben die Option.
- 7 Wenn Sie mehr Informationen zu einem einzelnen User erfahren möchten, klicken Sie in der Spalte **Name** auf den entsprechenden User. Weitere Informationen finden Sie in Kapitel 4.5.

Der Bereich „**Attributes**“ zeigt, welche Eigenschaften eine Gruppe besitzt. Gruppenattribute kommen bei der Konfiguration nicht zum Einsatz.

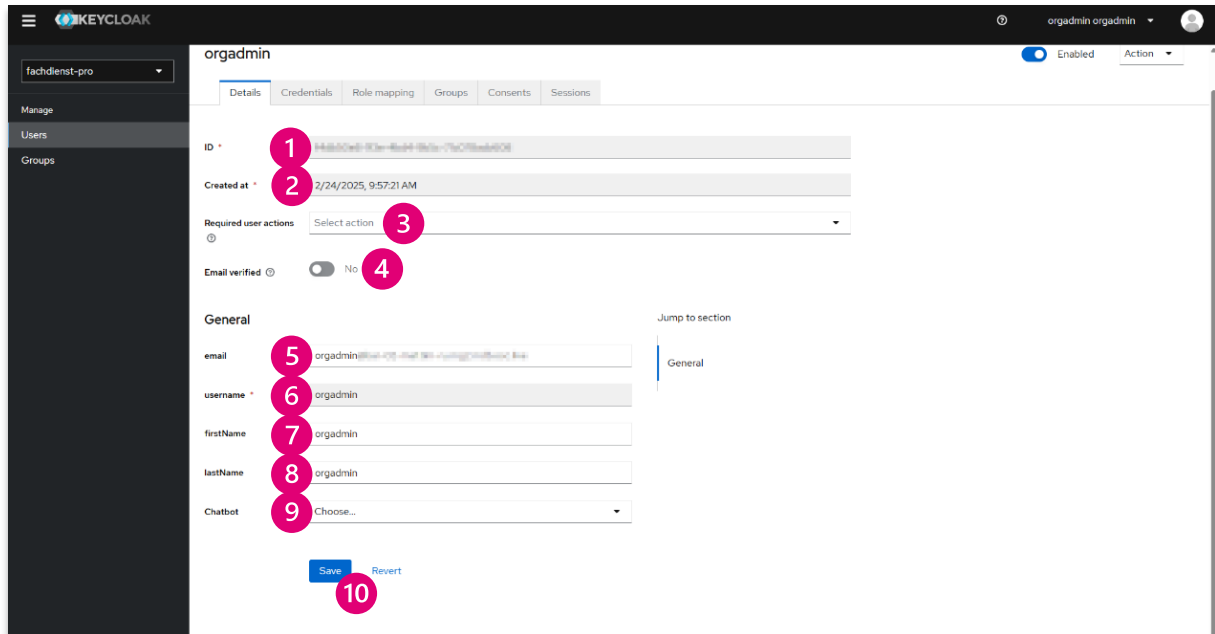


1 Klicken Sie auf den Reiter **[Attributes]**.

Aus sicherheitstechnischen Gründen können Sie in dem Bereich nichts verändern.

4.5 KeyCloak: Detailinformationen User

Durch Klicken auf einen einzelnen User wie in Kapitel 4.4 beschrieben, gelangen Sie zu einer Detailübersicht des ausgewählten Users.



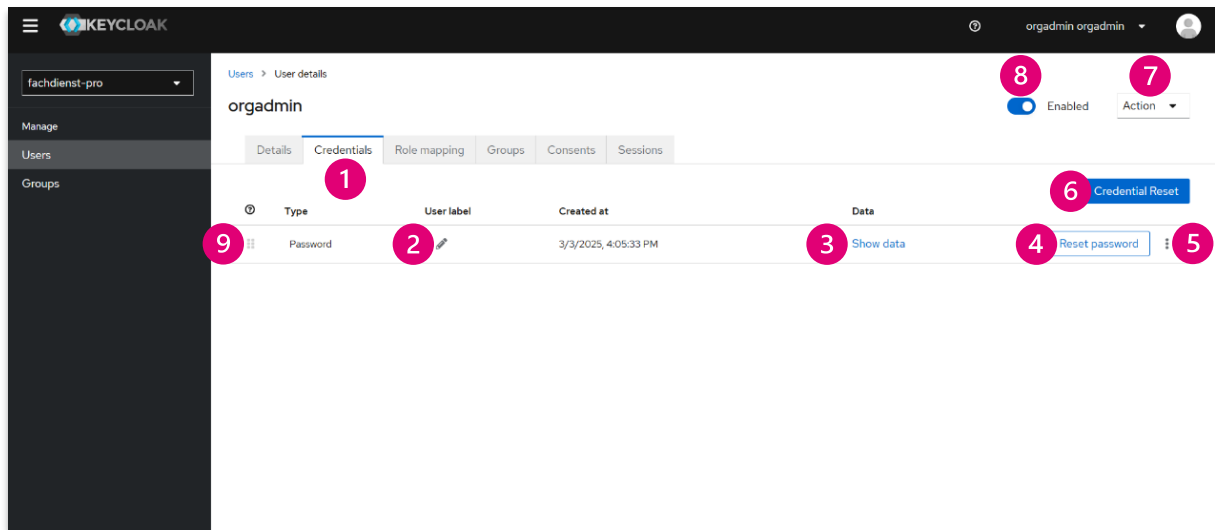
- 1 Im Feld **ID** wird Ihnen die einzigartige ID des Nutzers angezeigt. Dieses Feld dient lediglich der Anzeige. Sie können die ID nicht verändern.
- 2 Das Feld **Created at** zeigt Ihnen an, wann dieser Account erstellt worden ist. Dieses Feld dient lediglich der Anzeige. Sie können das Datum nicht verändern.
- 3 Wenn Sie auf das Feld **Required user actions** klicken, öffnet sich ein Drop-Down-Menü mit folgenden Optionen:
 - **Configure OTP:** Erfordert die Einrichtung eines mobilen Passwortgenerators;
 - **Update Password:** Erfordert die Eingabe eines neuen Passworts;
 - **Update Profile:** Erfordert die Eingabe neuer persönlicher Daten;
 - **Verify Email:** Sendet dem Benutzer eine E-Mail, um seine E-Mail-Adresse zu bestätigen;
 - **Webauthn Register:** Alternativen für die 2FA, um diese neu oder initial einzurichten;
 - **Verify Profile:** Verifizieren Sie Ihr Profil.

Die folgenden Optionen erfüllen im TI-Messenger keinen Zweck:

- Webauthn Register Passwordless;
 - Update User Locale.
- 4 Mit dem **Schieberegler** können Sie angeben, ob die E-Mail dieses Users bereits verifiziert wurde oder nicht.

- 5 Im Feld **E-Mail** ist bereits eine E-Mail-Adresse oder der Proxy, mit dem Sie sich angemeldet haben, hinterlegt. In diesem Feld müssen Sie nur tätig werden, wenn Sie die E-Mail-Adresse bzw. den Proxy ändern wollen oder überhaupt erst eintragen müssen.
- 6 Im Feld **Username** steht der Name des User, der nicht verändert werden kann.
- 7 Im Feld **firstName** geben Sie den Vornamen des Users ein.
- 8 Im Feld **lastName** geben Sie den Nachnamen des Users ein.
- 9 Im Feld **Chatbot** können Sie auswählen, ob der von Ihnen angelegt User ein Chatbot ist oder nicht.
- 10 Wenn Sie alles aufgefüllt oder Änderungen vorgenommen haben, klicken Sie abschließend auf den Button **[Save]**, um die Daten abzuspeichern. Falls Sie den Vorgang abbrechen möchten, klicken Sie auf den Button **[Revert]**.

4.5.1 KeyCloak: User Credentials

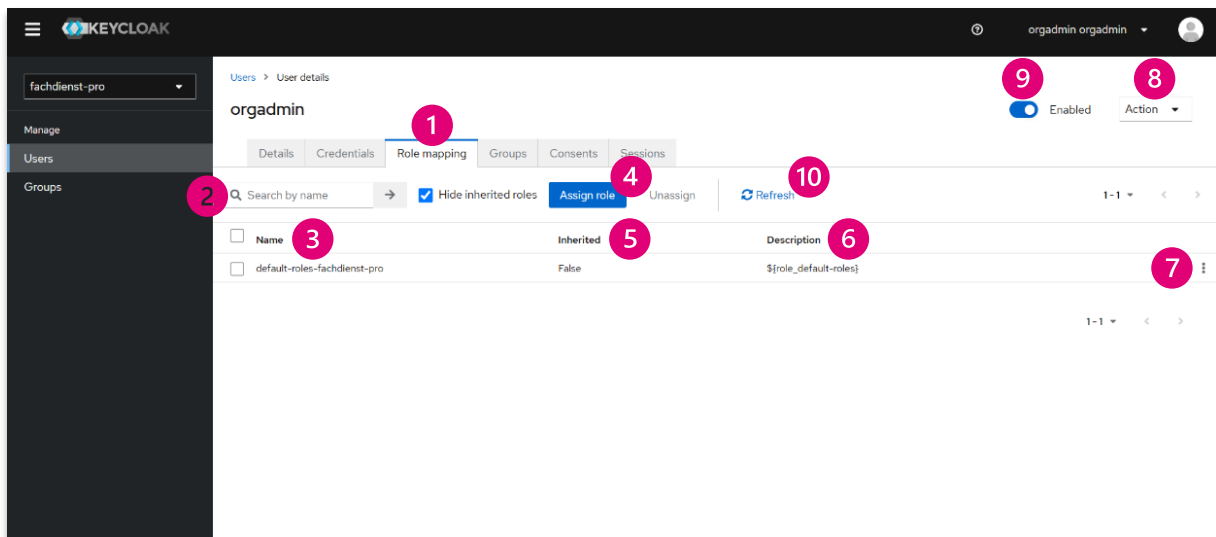


- 1 Klicken Sie auf den Reiter **[Credentials]**, um die Credentials des Users zu bearbeiten. Sie erhalten eine Übersicht zu den Credentials des Users. Es öffnet sich eine Tabelle mit folgenden Spalten:
 - **Type:** In dieser Spalte ist beschrieben, um welche Art des Passwortes es sich handelt;
 - **User label:** Dies ist eine zuweisbare Bezeichnung zur Erkennung der Anmeldeinformationen, wenn diese bei der Anmeldung als Auswahloption angezeigt werden. Sie kann auf einen beliebigen Wert zur Beschreibung der Anmeldeinformationen gesetzt werden. Diese Möglichkeit ist allerdings im TI-Messenger global abgeschaltet worden;
 - **Created at:** Zeigt an, wann das Passwort erstellt wurde;
 - **Data:** Klicken Sie auf den Button **[Show Data]**, um weitere Daten zu Ihrem Passwort zu erhalten.
- 4 Am Ende jeder Zeile befindet sich der Button **[Reset password]**. Klicken Sie auf den Button, um Ihr Passwort zu ändern.
- 5 Rechts neben dem Button **[Reset password]** befindet sich ein **Drei-Punkte-Menü**. Klicken Sie darauf, um die Option erhalten, diese Credentials zu löschen.
- 6 Wenn Sie sämtliche Credentials zurücksetzen möchten, klicken Sie auf den Button **[Credential Reset]**.
- 7 Wenn Sie auf das Feld **[Action]** klicken, öffnet sich ein Drop-Down-Menü mit folgenden Optionen:
 - **Impersonate:** Diese Option wurde aus Sicherheitsgründen deaktiviert;
 - **Delete:** Durch Klicken auf diese Option löschen Sie den User.
- 8 Über der Übersicht befindet sich ein **Schieberegler**. Durch Verschieben dieses Reglers deaktivieren Sie den Account ohne ihn zu löschen.

9

Mit den **Handlern** der obersten Ebene können Sie die Priorität der Anmeldeinformationen für den Benutzer ändern. Die obersten Anmeldeinformationen haben die höchste Priorität. Mit den Handlern in einem erweiterbaren Bereich können Sie die visuelle Reihenfolge der Anmeldeinformationen ändern. Die obersten Anmeldeinformationen werden ganz links angezeigt.

4.5.2 KeyCloak: User Role mapping



1 Klicken Sie auf den Reiter **[Role mapping]**, um die Rollen und die Zugehörigkeiten des Users einzusehen und zu bearbeiten.

2 Wenn Sie nach einer bestimmten Rolle suchen wollen, können Sie Ihre Suchanfrage in das Suchfeld **[Search by name]** eingeben.

Sie erhalten eine Übersicht zu den Rollen des Users. Es öffnet sich eine Tabelle mit folgenden Spalten:

3 • **Name:** In dieser Spalte steht die Rolle, die der User hat. Links neben jedem Rollennamen befindet sich eine Checkbox. Durch Anklicken der Checkbox in der jeweiligen Spalte können Sie eine oder mehrere Rollen auswählen:

4 • **Assign:** Sie können dem User bestimmte Rollen neu zuweisen. Klicken Sie hierfür auf den Button **[Assign role]** und wählen Sie die entsprechende neue Rolle aus;

• **Unassign:** Haben Sie eine oder mehrere Rollen ausgewählt, öffnet sich der Button **[Unassign]**. Dadurch können Sie die Zuweisung einer bestimmten Rolle wieder aufheben;

5 • **Inherited:** In dieser Spalte wird Ihnen angezeigt, ob die Rolle des Users geerbt wurde;

6 • **Description:** Eine kurze Beschreibung der Rolle.

7 Wenn Sie die Zuweisung einer einzelnen Rolle entfernen wollen, befindet sich am Ende einer jeden Zeile das **3-Punkte Menü**. Wenn Sie das Anklicken eröffnet sich die Option **[Unassign]** und können damit die Zuweisung aufheben. Sollten Sie sich anders entscheiden klicken Sie neben die Option.

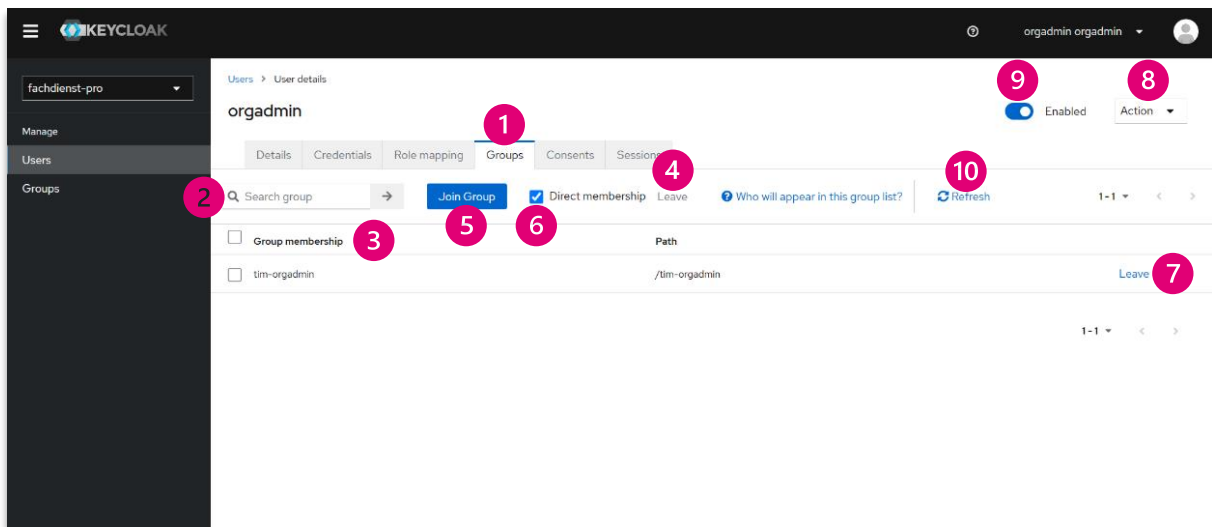
8 Wenn Sie auf das Feld **[Action]** klicken, öffnet sich ein Drop-Down-Menü mit folgenden Optionen:

• **Impersonate:** Diese Option wurde aus Sicherheitsgründen deaktiviert;

• **Delete:** Durch Klicken auf diese Option löschen Sie den User.

- 9 Über der Übersicht befindet sich ein **Schieberegler**. Durch Verschieben dieses Reglers deaktivieren Sie den Account ohne ihn zu löschen.
- 10 Um die Ergebnisse zu aktualisieren, klicken Sie auf den Button **[Refresh]**.

4.5.3 KeyCloak: User Groups

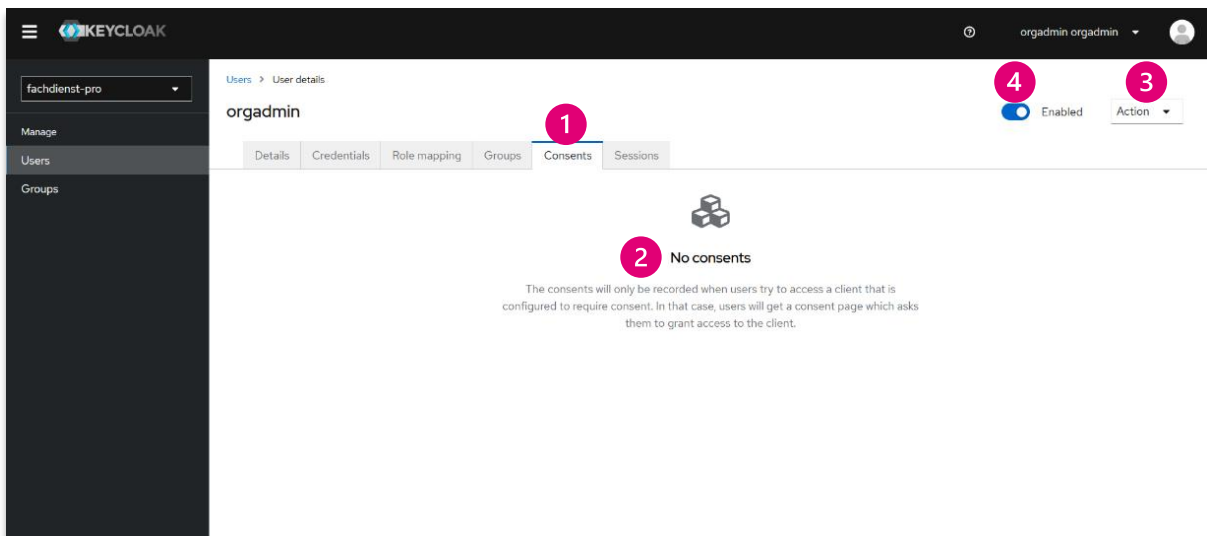


Durch Klicken auf einen **einzelnen User** wie in Kapitel 4.1 gelangen Sie zu einer Detailübersicht des ausgewählten Users.

- 1 Klicken Sie auf den Reiter **[Groups]**, um die Gruppen und die Mitgliedschaft von Gruppen des Users zu einzusehen und zu bearbeiten.
- 2 Wenn Sie nach einer bestimmten Gruppe suchen wollen, können Sie Ihre Suchanfrage in das Suchfeld **[Search group]** eingeben. Sie erhalten eine Übersicht über die Gruppen des Users in Form einer Tabelle mit den folgenden Spalten:
 - 3
 - **Group membership:** In dieser Spalte sehen Sie den Namen der Gruppe, in der der User Mitglied ist. Links neben jeder Gruppenmitgliedschaft befindet sich eine **Checkbox**. Durch Anklicken der Checkbox in der jeweiligen Spalte können Sie eine oder mehrere Gruppenmitgliedschaften auswählen.
 - 4
 - **Leave:** Wenn Sie eine oder mehrere Gruppen ausgewählt haben, öffnet sich durch bedingte Aktivierung der Button **[Leave]**. Dadurch können Sie aus den zuvor ausgewählten Gruppen austreten.
 - **Path:** In dieser Spalte wird Ihnen ein Teil des Pfades angezeigt, der für die URL relevant ist. Dies dient nur der Information und Sie können nichts daran verändern.
- 5 Durch Klicken auf den Button **[Join Group]** können Sie weitere Gruppen auswählen, denen Sie beitreten möchten.
- 6 Direkt rechts neben dem Button **[Join Group]** befindet sich ein Kontrollkästchen mit der Einstellung **Direct membership**. Standardmäßig ist ausgewählt, dass Ihnen nur Gruppen angezeigt werden, in denen Sie direktes Mitglied sind. Sie können den Haken im **Kontrollkästchen** durch Anklicken entfernen. Damit werden Ihnen auch Gruppenmitgliedschaften angezeigt, bei denen Sie nicht direktes Mitglied sind.

- 7 Wenn Sie aus einer einzelnen Gruppe austreten möchten, befindet sich am Ende einer jeden Zeile die Option **[Leave]**. Klicken Sie auf den Button um die Gruppe zu verlassen.
- 8 Wenn Sie auf das Feld **[Action]** klicken, öffnet sich ein Drop-Down-Menü mit folgenden Optionen:
 - **Impersonate**: Diese Aktion steht Ihnen aus Sicherheitsgründen nicht zur Verfügung;
 - **Delete**: Durch Klicken auf diese Option können Sie den User löschen.
- 9 Über der Übersicht befindet sich ein **Schieberegler**. Durch das Verschieben dieses Reglers deaktivieren Sie den Account ohne ihn zu löschen.
- 10 Um die Ergebnisse zu aktualisieren, klicken Sie auf den Button **[Refresh]**.

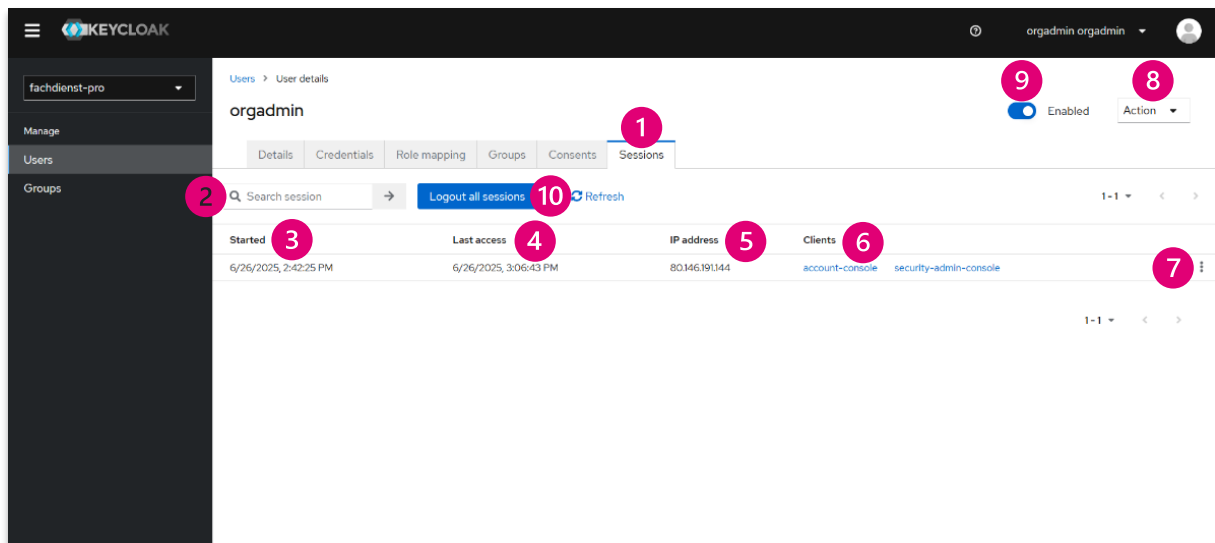
4.5.4 KeyCloak: User Consents



Durch das Klicken auf einen **einzelnen User** wie in Kapitel 4.4 beschrieben gelangen Sie zu einer Detailübersicht des ausgewählten Users.

- 1 Klicken Sie auf den Reiter **[Consents]**, erhalten Sie eine Übersicht zu Anfragen zur Einwilligung der Nutzung von Clients.
- 2 Die Einwilligungen werden nur dann erfasst, wenn Nutzer versuchen, auf einen Client zuzugreifen, der so konfiguriert ist, dass dafür eine Einwilligung erforderlich ist. In diesem Fall wird den Nutzern eine Einwilligungsseite angezeigt, auf der sie aufgefordert werden, den Zugriff auf den Client zu gewähren.
- 3 Wenn Sie auf das Feld **[Action]** klicken, öffnet sich ein Drop-Down-Menü mit folgenden Optionen:
 - **Impersonate:** Diese Aktion steht Ihnen aus Sicherheitsgründen nicht zur Verfügung;
 - **Delete:** Durch Klicken auf diese Option können Sie den User löschen.
- 4 Über der Übersicht befindet sich ein **Schieberegler**. Durch das Verschieben dieses Reglers können Sie den Account deaktivieren ohne ihn zu löschen.

4.5.5 KeyCloak: User Sessions



Durch das Klicken auf einen **einzelnen User** wie in Kapitel 4.4 beschrieben gelangen Sie zu einer Detailübersicht des ausgewählten Users.

- 1 Klicken Sie auf den Reiter **[Sessions]** um einzusehen, welche Sessions (Sitzungen) über den User laufen.
- 2 Wenn Sie nach einer bestimmten Sitzung suchen wollen, können Sie Ihre Suchanfrage in das Suchfeld **[Search session]** eingeben.

Sie erhalten eine Übersicht zu allen Sessions des Users. Es öffnet sich eine Tabelle mit den folgenden Spalten:

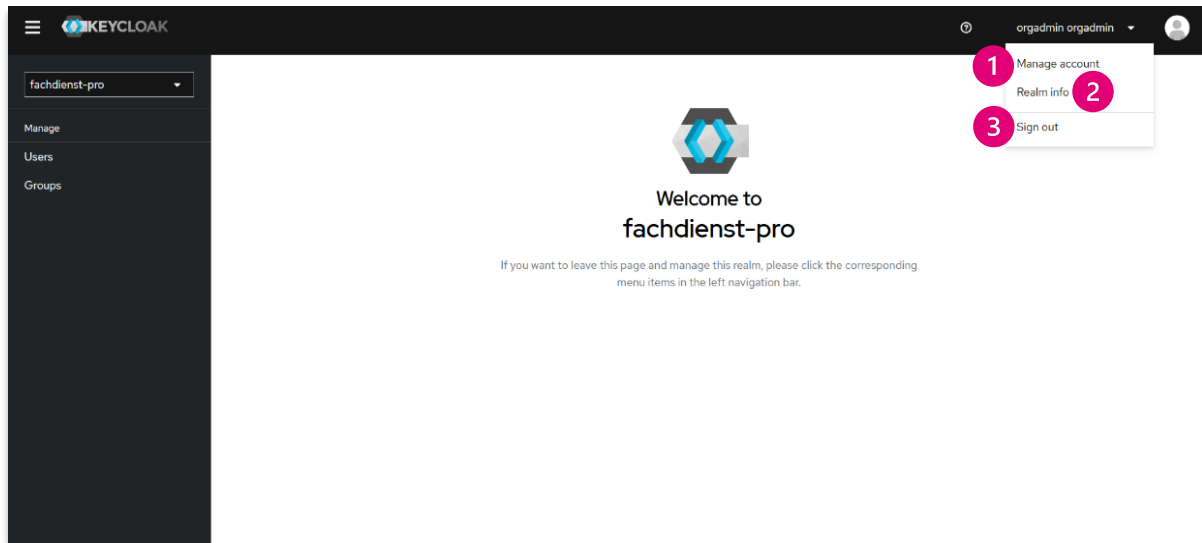
- 3
 - **Started:** Information darüber, wann die jeweilige Session vom User gestartet wurde. Diese Spalte dient lediglich der Anzeige und ihr Inhalt kann nicht verändert werden;
- 4
 - **Last access:** Information darüber, wann vom User das letzte Mal auf die jeweilige Session zugegriffen wurde. Diese Spalte dient lediglich der Anzeige und ihr Inhalt kann nicht verändert werden;
- 5
 - **IP address:** Information darüber, über welche IP-Adresse die Sitzung läuft. Diese Spalte dient lediglich der Anzeige und ihr Inhalt kann nicht verändert werden;
- 6
 - **Clients:** Information darüber, auf welche Konsolen Sie Zugriff haben:
 - account-console: Konsole für Nutzeranmeldungsdaten,
 - security-admin-console: Verwaltung aller Accounts für die Rolle Org-Admin.
- 7 Wenn Sie die Sitzung eines Users beenden möchten, befindet sich am Ende einer jeden Zeile das **Drei-Punkte Menü**. Durch Anklicken öffnet sich die Option **[Sign out]**, mit der Sie die Sitzung beenden können.
- 8 Wenn Sie auf das Feld **[Action]** klicken, öffnet sich ein Drop-Down-Menü mit folgenden Optionen:

- **Impersonate:** Diese Aktion steht Ihnen aus Sicherheitsgründen nicht zur Verfügung;
- **Delete:** Durch das Klicken auf diese Option können Sie den User löschen.

9 Über der Übersicht befindet sich ein **Schieberegler**. Durch das Verschieben dieses Reglers können Sie den Account deaktivieren ohne ihn zu löschen.

10 Wenn Sie alle Sessions eines Users beenden möchten, klicken Sie auf den Button **[Logout all sessions]**. Wenn Sie die Ergebnisse aktualisieren wollen, klicken Sie auf den Button **[Refresh]**.

4.6 KeyCloak: Einstellungen zum eigenen User



Klicken Sie auf Ihren Namen oben rechts in der Ecke. Es öffnet sich ein **Drop-Down Menü** mit folgenden Optionen:

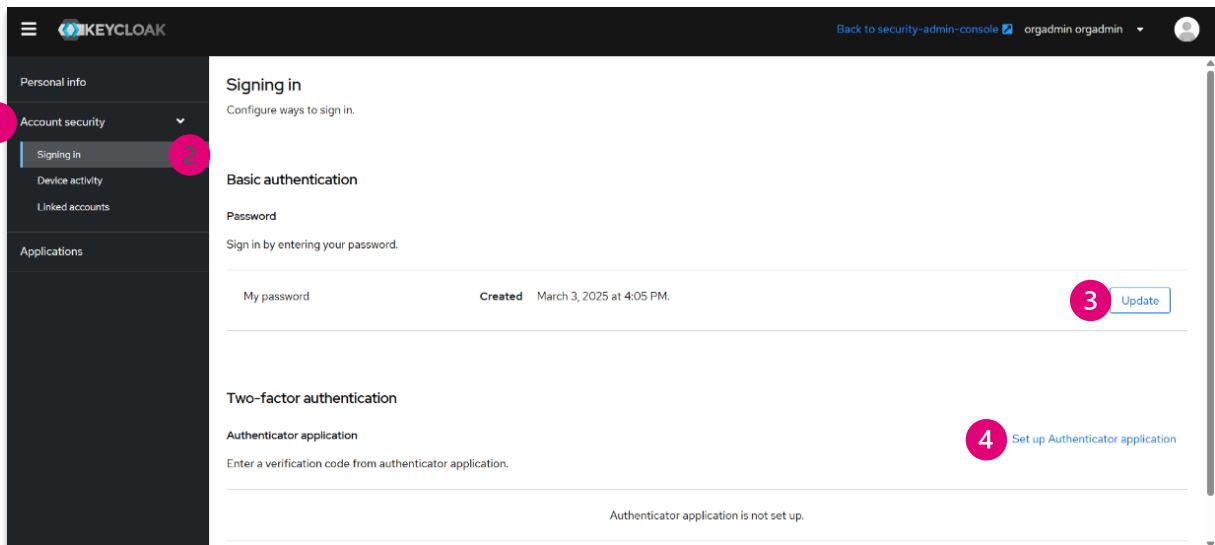
- 1 Um Ihren eigenen Account zu verwalten, klicken Sie auf die Option **[Manage Account]**. Weitere Informationen erhalten Sie in den Kapiteln 4.6.1 bis 4.6.5.
- 2 Der Button **[Realm Info]** bringt Sie zurück zur Startseite von KeyCloak fachdienst-pro.
- 3 Um den Bereich zu verlassen, klicken Sie auf die Option **[Sign out]**.

4.6.1 Keycloak: Manage account – Personal info

The screenshot shows the Keycloak user management interface. On the left sidebar, the 'Personal info' menu item is highlighted with a red circle '1'. The main content area is titled 'Personal info' and 'Manage your basic information'. Under the 'General' section, there are five input fields: 'email' (2) containing 'orgadmin@bar-02-mal.tim-ru.mg2.mdb.osc.live', 'username' (3) containing 'orgadmin', 'firstName' (4) containing 'orgadmin', 'lastName' (5) containing 'orgadmin', and a 'Chatbot' dropdown (6) with 'Choose...' selected. At the bottom of the form are two buttons: a blue 'Save' button (7) and a grey 'Cancel' button (8). On the right side, there is a 'Jump to section' dropdown menu with 'General' selected.

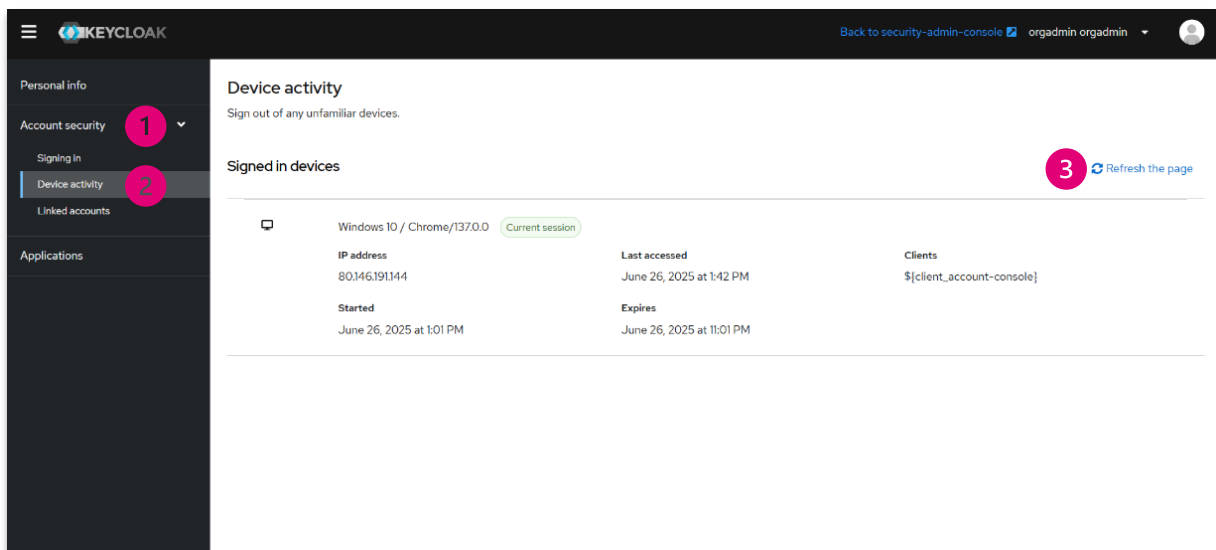
- 1 Sie befinden sich im Bereich **Personal info** Ihres eigenen Accounts.
- 2 Im Feld **E-Mail** ist bereits eine E-Mail-Adresse oder der Proxy, mit dem Sie sich angemeldet haben, hinterlegt. In diesem Feld müssen Sie nur tätig werden, wenn Sie die E-Mail-Adresse oder den Proxy ändern wollen.
- 3 Im Feld **Username** steht der Name des Users und kann nicht verändert werden.
- 4 Im Feld **firstname** steht der Vorname des Users und kann nicht verändert werden.
- 5 Im Feld **lastname** steht der Nachname des Users und kann nicht verändert werden.
- 6 Im Feld **Chatbot** können Sie auswählen, ob der von Ihnen angelegte User ein Chatbot ist oder nicht.
- 7 Um alle Änderungen zu speichern, klicken Sie auf den Button **[Save]**.
- 8 Um den Vorgang abzubrechen, klicken Sie auf den Button **[Cancel]**.

4.6.2 KeyCloak: Manage account – Signing in



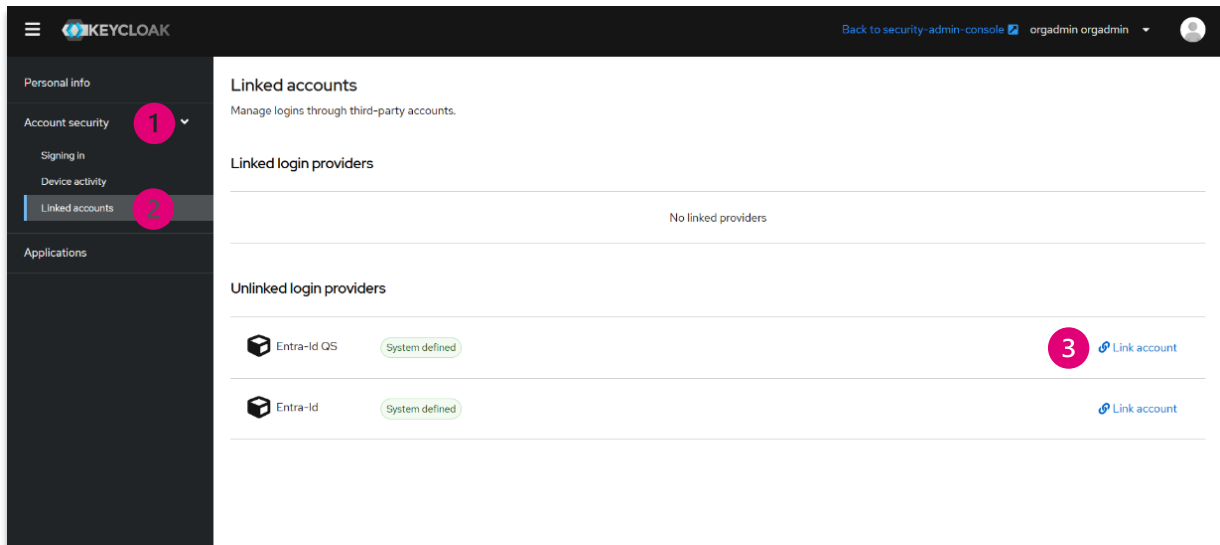
- 1 Sie befinden sich im Bereich **Account security** Ihres eigenen Accounts.
- 2 Der Bereich **Account security** ist in drei Abschnitte aufgeteilt. Durch Klicken auf den Abschnitt **Signing in** können Sie Login-Optionen konfigurieren. Die standardmäßige Einstellung für den Login ist die Eingabe eines Passwortes.
- 3 Im Abschnitt **Password** kann das eigene Passwort durch Klicken auf den Button **[Update]** verändert / aktualisiert werden.
- 4 Im Abschnitt **Two-factor authentication** können Sie die Zwei-Faktor Authentifizierung einrichten. Durch Klicken auf den Absprung **Set up Authenticator application** werden Sie zu einer Anleitung für die Einrichtung der Zwei-Faktor Authentifizierung weitergeleitet.

4.6.3 KeyCloak: Manage account – Device Activity



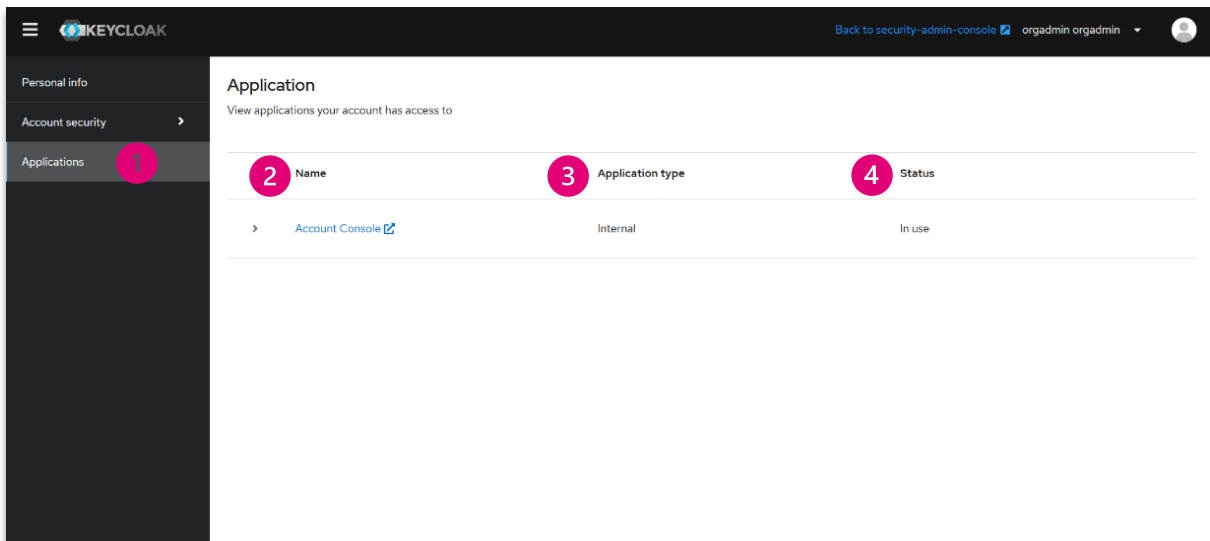
- 1 Sie befinden sich im Bereich **Account security** Ihres eigenen Accounts.
- 2 Der Bereich **Account security** ist aufgeteilt in drei Unterbereiche. Durch Klicken auf den Bereich **Device activity** können Sie für Ihr aktuelles Gerät verschiedene Informationen zu Ihrer Sitzung einsehen. Sie erhalten folgende Informationen:
 - **IP address:** Information darüber, über welche IP-Adresse die Sitzung läuft. Diese Information dient lediglich der Anzeige und ihr Inhalt kann nicht verändert werden;
 - **Started:** Information darüber, wann die jeweilige Session vom User gestartet wurde. Diese Information dient lediglich der Anzeige und ihr Inhalt kann nicht verändert werden;
 - **Last accessed:** Information darüber, wann vom User das letzte Mal auf die jeweilige Session zugegriffen wurde. Diese Information dient lediglich der Anzeige und ihr Inhalt kann nicht verändert werden;
 - **Expires:** Information darüber, wann die Sitzung ausläuft. Diese Information dient lediglich der Anzeige und ihr Inhalt kann nicht verändert werden;
 - **Clients:** Information darüber, auf welcher Konsole in dieser Sitzung zugegriffen wurde.
- 3 Wenn Sie die Ergebnisse aktualisieren wollen, klicken Sie auf den Button **[Refresh the page]**.

4.6.4 KeyCloak: Manage account – Linked accounts



- 1 Sie befinden sich im Bereich **Account security** Ihres eigenen Accounts.
- 2 Der Bereich **Account security** ist aufgeteilt in drei Unterbereiche. Durch Klicken auf den Bereich **Linked accounts** können Sie die Anmeldungen über Konten von Drittanbietern verwalten. Der Bereich teilt sich in zwei Unterbereiche:
 - **Linked login providers:** Information darüber, ob und welche Login-Anbieter verlinkt bzw. verknüpft sind;
 - **Unlinked login providers:** Information darüber, ob und welche Login-Anbieter nicht verlinkt bzw. verknüpft sind.
- 3 Wenn Sie einen der noch nicht verknüpften Login-Anbieter anbinden möchten, klicken Sie in der jeweiligen Zeile auf den Button **[Link account]**.

4.6.5 KeyCloak: Manage account – Applications

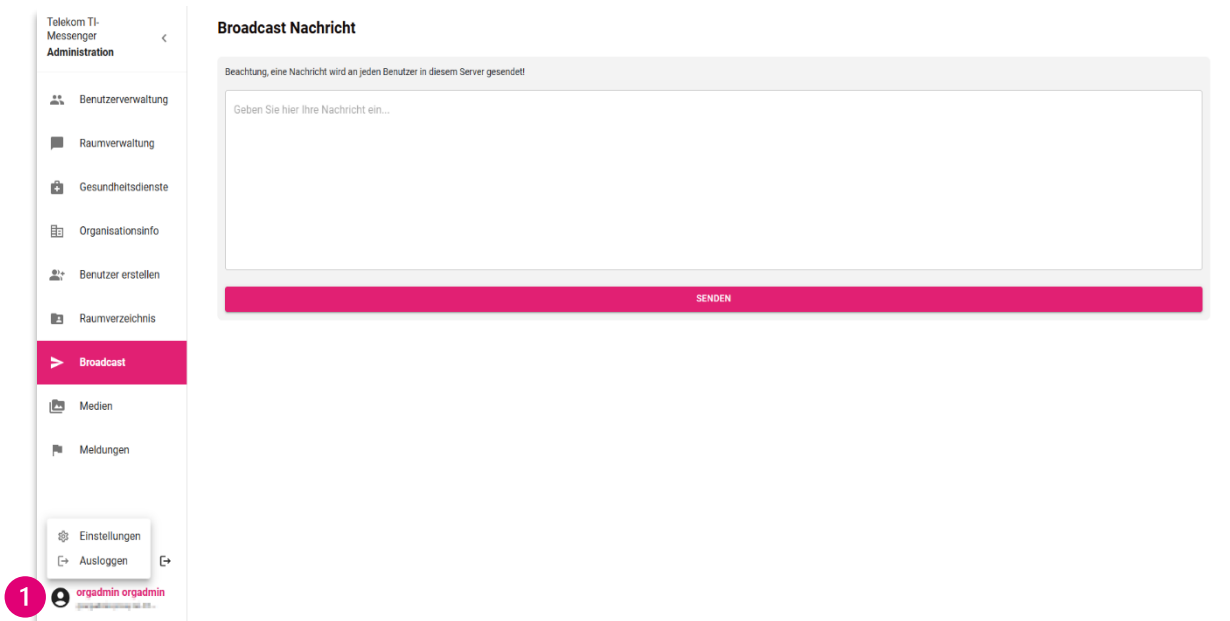


- 1 Sie befinden sich im Bereich **Applications** Ihres eigenen Accounts. Der Bereich **Applications** zeigt Ihnen Anwendungen an, auf die Ihr Konto Zugriff hat. Die Übersicht gestaltet sich wie folgt:
- 2
 - **Name:** Information darüber, auf welche Applikation Sie mit Ihrem aktuellen Konto Zugriff haben;
- 3
 - **Application type:** Information über die Art die Applikation;
- 4
 - **Status:** Information über den Status der Applikation.

5 Mein Account

In diesem Kapitel erhalten Sie umfassende Informationen zu Ihrem Account im Org-Admin des TI-Messengers. Sie lernen, wie Sie Ihr Profil verwalten und anpassen, einschließlich der Optionen zur Änderung Ihres Profilbilds, zur Aktualisierung Ihres Passworts und zur Anpassung Ihrer Einstellungen. Zusätzlich erfahren Sie, wie Sie die verschiedenen Sicherheits- und Datenschutzoptionen nutzen können, um Ihr Benutzererlebnis zu optimieren und die Sicherheit Ihrer Daten zu gewährleisten. Die Übersichtlichkeit dieser Funktionen sowie die Möglichkeit zur individuellen Anpassung ermöglichen es Ihnen, Ihr Benutzerkonto effizient zu verwalten.

In der linken unteren Ecke des Bildschirms werden Ihr Profilbild, Ihr Anzeigename und Ihre TI-Messenger-ID angezeigt.



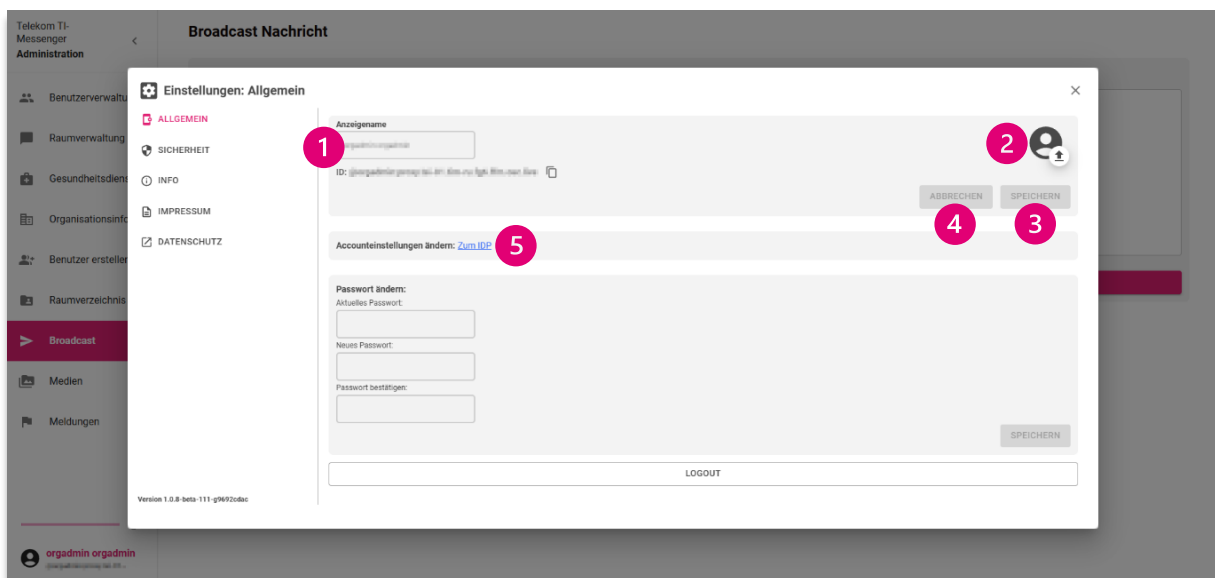
- 1 Klicken Sie auf Ihr **Profilbild** bzw. Ihren **Username**, um zwischen „Einstellungen“ und „Ausloggen“ auszuwählen.

5.1 Einstellungen

Nachdem Sie im vorherigen Schritt „Einstellungen“ ausgewählt haben, öffnet sich ein neues Fenster, in dem Sie zahlreiche Anpassungsmöglichkeiten für Ihr Benutzerkonto finden. Die individuellen Einstellungen erlauben es Ihnen, den Org-Admin-Client nach Ihren Bedürfnissen zu konfigurieren, um die Benutzerfreundlichkeit, Sicherheit und Effizienz zu optimieren. Durch gezielte Anpassungen können Sie Ihr Benutzererlebnis verbessern und sicherstellen, dass der TI-Messenger optimal auf Ihre Anforderungen abgestimmt ist.

5.1.1 Einstellungen: Allgemein

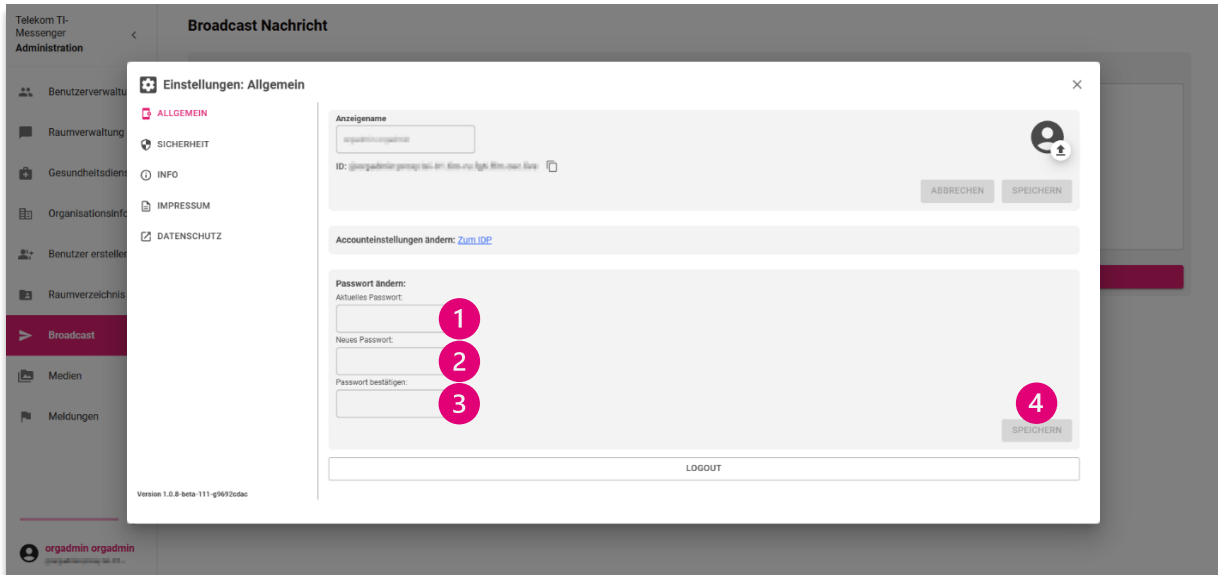
Im Reiter **[Allgemein]** haben Sie die Möglichkeit, Ihr Profilbild zu ändern, Ihr Passwort zurückzusetzen und Ihre TI-Messenger-ID einzusehen. Möchten Sie Ihren Benutzernamen anpassen, können Sie dies wie bei jedem anderen Nutzer tun. Zudem finden Sie hier allgemeine Informationen zu Ihrem Account sowie Optionen zu Sicherheit, Datenschutz, Informationen und das Impressum.



- 1 Der **[Anzeigename]** zeigt Ihren aktuellen Benutzernamen an, der nicht verändert werden kann.
- 2 Um Ihr Profilbild zu ändern, klicken Sie auf den **Pfeil** neben dem Bild in der oberen rechten Ecke.
- 3 Nachdem Sie ein neues Profilbild hochgeladen haben, bestätigen Sie die Änderung mit einem Klick auf **[Speichern]**.
- 4 Wenn Sie den Vorgang abbrechen möchten, klicken Sie auf den Button **[Abbrechen]**.
- 5 Falls Sie Änderungen an Ihren Accounteinstellungen vornehmen möchten, können Sie über den Link **[Zum IDP]** zur Seite des Fachdienstes Pro gelangen, wodurch Sie den Org-Admin-Bereich verlassen.

5.1.2 Passwort ändern

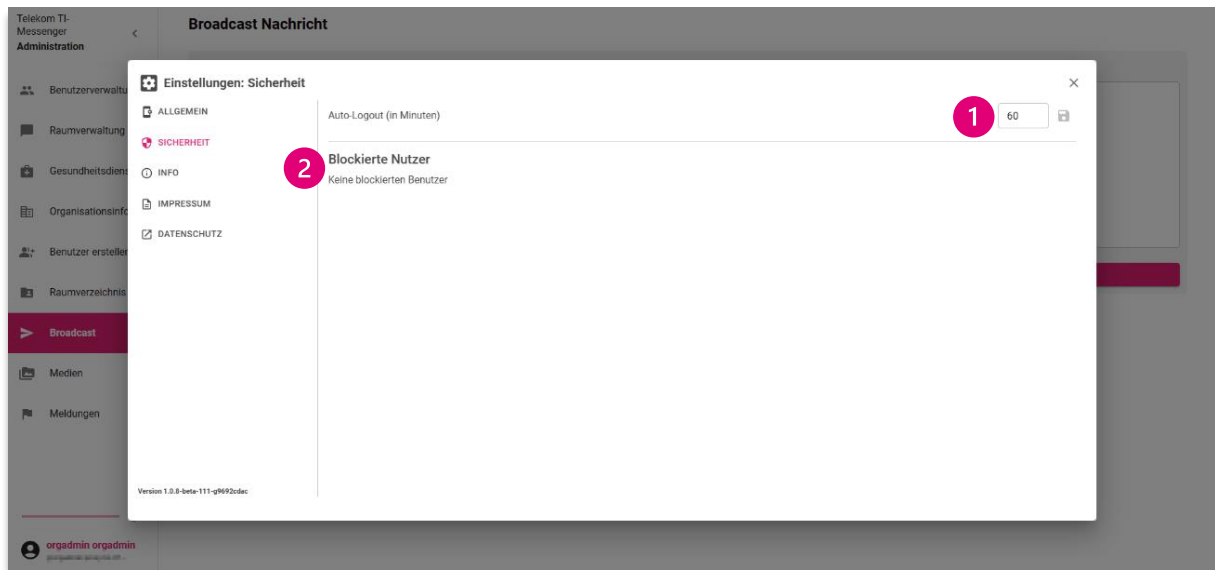
Ein regelmäßiger Passwortwechsel verringert das Risiko eines unbefugten Zugriffs, insbesondere wenn Ihre Anmeldedaten möglicherweise kompromittiert wurden. Durch diese Maßnahme erhöhen Sie die Sicherheit Ihrer Daten und schützen sich vor möglichem Missbrauch.



- 1 Bitte geben Sie zunächst Ihr **aktuelles Passwort** ein.
- 2 Anschließend tragen Sie Ihr **neues Passwort** in das vorgesehene Feld ein.
- 3 Zur Bestätigung geben Sie hier bitte Ihr **neues Passwort** erneut ein.
- 4 Um Ihre Änderungen zu speichern, klicken Sie abschließend auf **[Speichern]**.

5.1.3 Einstellungen: Sicherheit

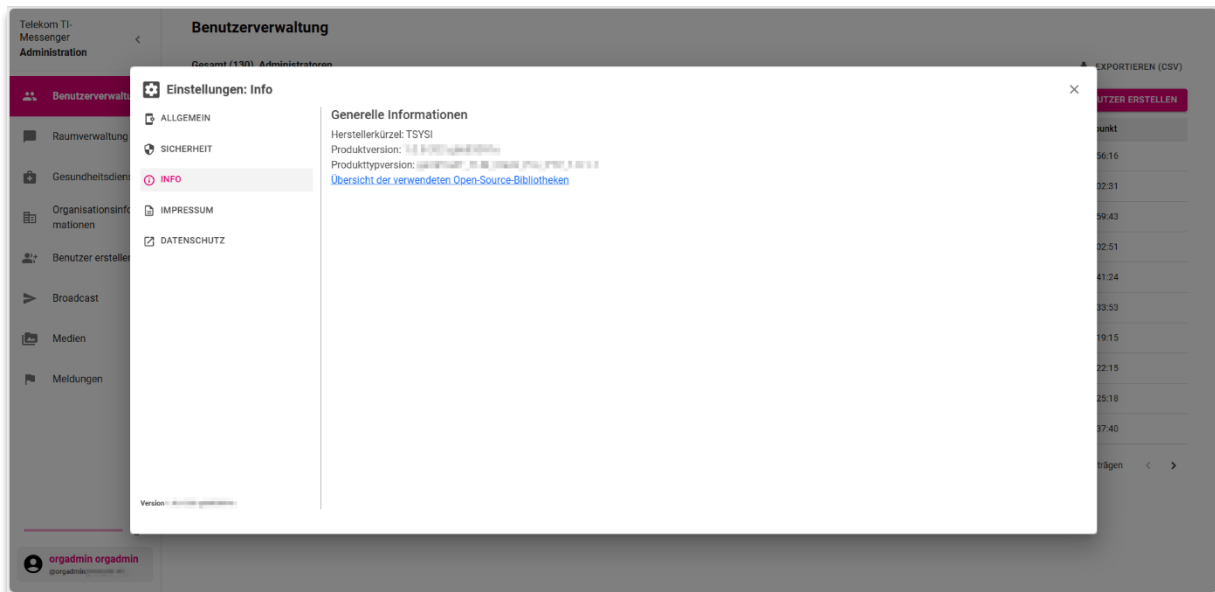
Im Bereich „Sicherheit“ haben Sie die Möglichkeit, Einstellungen vorzunehmen, die Ihre Privatsphäre und den Schutz Ihrer Daten im TI-Messenger erhöhen.



- 1 Klicken Sie auf **[Sicherheit]**, erhalten Sie die Möglichkeit den automatischen Logout anzupassen. Sie werden nach 60 Minuten automatisch ausgeloggt. Diesen Wert können Sie selbst abändern, sodass sie eher oder später automatisch abgemeldet werden. Dafür klicken Sie in das Feld, in dem die Minutenanzahl steht, und ändern diese. Anschließend klicken Sie auf die Diskette daneben, um die Eingabe zu speichern.
- 2 Ebenfalls sehen Sie in diesem Bereich alle Nutzer, die Sie blockiert haben.

5.1.4 Einstellungen: Info

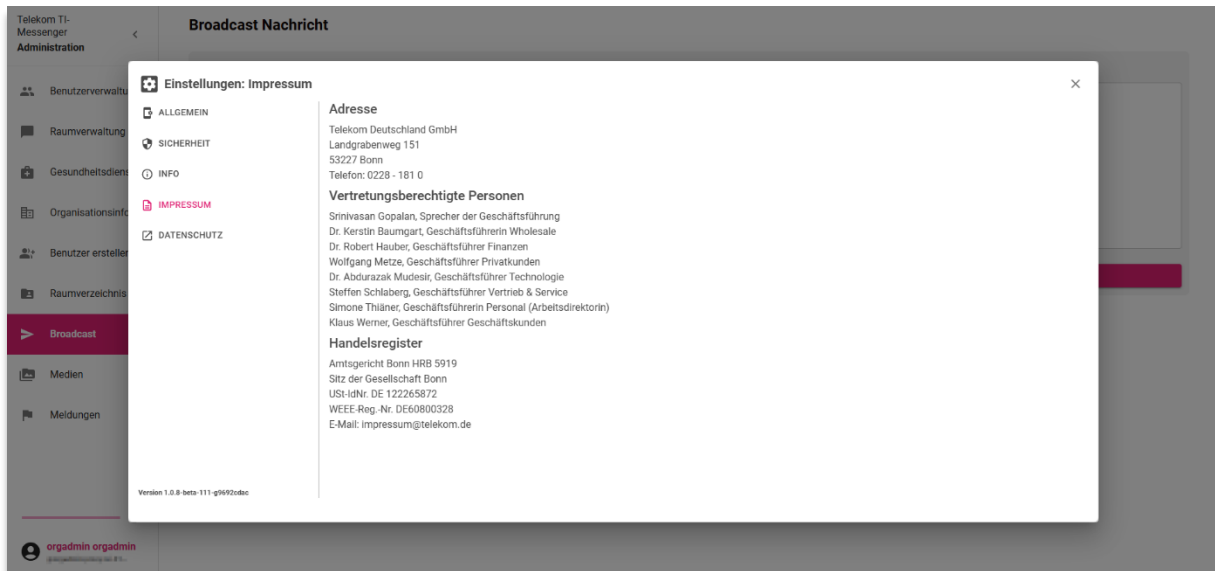
Im Bereich [Info] erhalten Sie grundlegende Informationen über das Herstellerkürzel sowie die aktuelle Version des Produkts, um Transparenz und Verständnis für die verwendete Software zu gewährleisten.



5.1.5 Einstellungen: Impressum

Im Impressum finden Sie wichtige rechtliche Informationen über den Anbieter des TI-Messengers, einschließlich der Firmenadresse und der vertretungsberechtigten Personen.

Klicken Sie auf **[Impressum]**, können Sie die Firmenadresse, vertretungsberechtigte Personen und Informationen zum Handelsregister einsehen.



5.1.6 Einstellungen: Datenschutz

Im Abschnitt [Datenschutz] finden Sie detaillierte Informationen darüber, welche personenbezogenen Daten erhoben und wie diese geschützt werden, um Ihre Privatsphäre sicherzustellen.

Bei diesem Reiter handelt es sich um einen Absprungpunkt, d. h. Sie werden zur externen Website der Telekom weitergeleitet, auf der Sie die Datenschutzhinweise der T-Systems International GmbH nachlesen können: <https://www.telekom.de/datenschutzhinweise/view/430.html>

Telekom TI-Messenger Administration

Broadcast Nachricht

Einstellungen: Impressum

- ALLGEMEIN
- SICHERHEIT
- INFO
- IMPRESSUM
- DATENSCHUTZ**

Adresse
Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn
Telefon: 0228 - 181 0

Vertretungsberechtigte Personen
Srinivasan Gopalan, Sprecher der Geschäftsführung
Dr. Kerstin Baumgart, Geschäftsführerin Wholesale
Dr. Robert Hauber, Geschäftsführer Finanzen
Wolfgang Metzke, Geschäftsführer Privatkunden
Dr. Abdurazak Mudesir, Geschäftsführer Technologie
Steffen Schlaberg, Geschäftsführer Vertrieb & Service
Simone Thilmer, Geschäftsführerin Personal (Arbeitsdirektorin)
Klaus Werner, Geschäftsführer Geschäftskunden

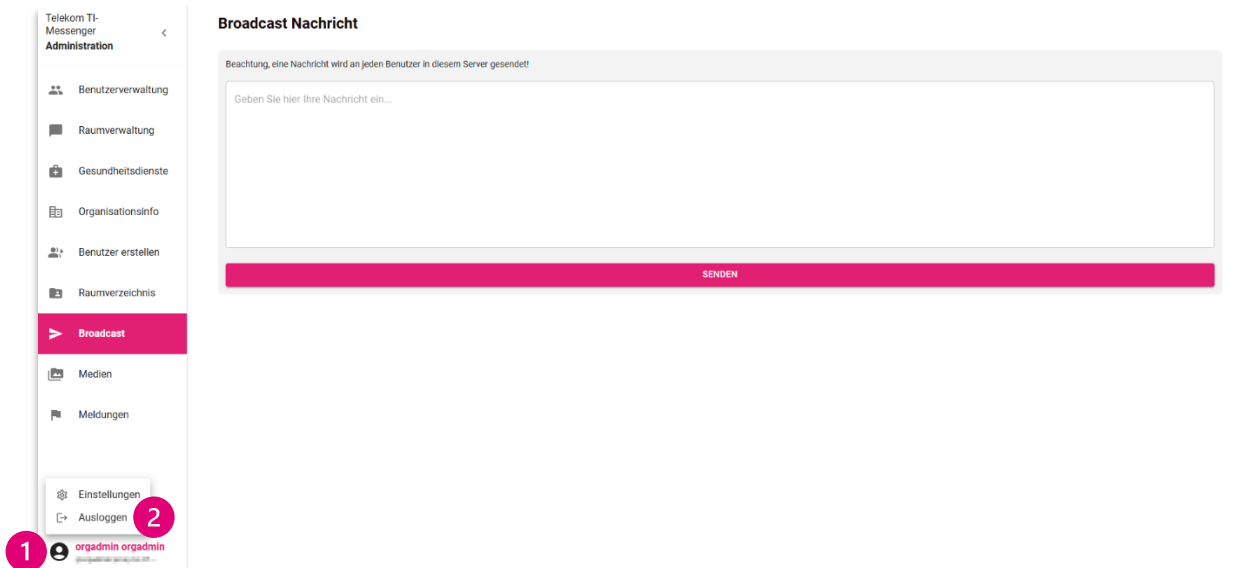
Handelsregister
Amtsgericht Bonn HRB 5919
Sitz der Gesellschaft Bonn
USt-IdNr. DE 122265872
WEEE-Reg.-Nr. DE60800328
E-Mail: impressum@telekom.de

Version 1.0.8-beta-111-q4692c0bc

orgadmin orgadmin

5.2 Ausloggen

In diesem Kapitel erfahren Sie, wie Sie sich sicher aus Ihrem Konto im Org-Admin-Client des TI-Messengers abmelden können. Das Ausloggen ist ein wichtiger Bestandteil der Sicherheit. Durch die korrekte Abmeldung schützen Sie Ihre persönlichen Daten und gewährleisten, dass unbefugte Zugriffe auf Ihr Konto verhindert werden. Hier finden Sie detaillierte Anweisungen, wie Sie den Abmeldevorgang einfach und schnell durchführen können.



- 1 Klicken Sie auf Ihr **Profilbild** bzw. Ihren **Username**, um die verfügbaren Optionen anzuzeigen.
- 2 Wählen Sie dann den Button **[Ausloggen]** aus, um sich von Ihrem Account abzumelden.

6 Passwortanforderungen

Beim Verwalten von Kennwörtern müssen die folgenden Sicherheitsanforderungen gemäß der BSI-Regelung „ORP.4.A22: Regelung zur Passwortqualität“ und BSI-Regelung „ORP.4.A8: Regelung des Passwortgebrauchs“ zwingend eingehalten werden. Diese Anforderungen sind darauf ausgelegt, Ihre Daten bestmöglich zu schützen und unbefugten Zugriff zu verhindern.

Um als sicher zu gelten, muss Ihr Passwort die folgenden Kriterien erfüllen:

- 1. Mindestlänge:** Das Passwort muss mindestens 14 Zeichen lang sein.
- 2. Zeichenklassen:** Das Passwort muss aus Zeichen aus mindestens drei der folgenden vier Zeichengruppen bestehen:
 - Kleinbuchstaben (a–z),
 - Großbuchstaben (A–Z),
 - Ziffern (0–9),
 - Erlaubte Sonderzeichen: \$ % + # - _
- 3. Nicht zulässig sind:**
 - Umlaute (ä, ö, ü) sowie Buchstaben, die nicht im deutschen Alphabet enthalten sind (z. B. ß, ê, ñ),
 - Andere Sonderzeichen, die nicht in der obigen Liste aufgeführt sind.

Beim Ändern eines Passworts ist sicherzustellen, dass das neue Kennwort sich von den fünf vorhergehenden Passwörtern unterscheidet. Dies stellt sicher, dass Ihre Sicherheitsmaßnahmen kontinuierlich aufrechterhalten werden, und minimiert das Risiko eines unbefugten Zugriffs auf Ihr Konto.

Des Weiteren gelten die Regelungen des Passwortgebrauchs (gemäß BSI-Grundschutz: ORP.4.A8):

- 1. Einsatz von Passwörtern als Authentifizierungsverfahren:** Es muss geprüft werden, ob Passwörter als alleinige Authentifizierung eingesetzt werden sollen oder durch weitere Verfahren wie z. B. Zertifikate oder Multi-Factor-Authentifizierung ergänzt bzw. ersetzt werden können.
- 2. Verbot der Wiederverwendung:** Passwörter dürfen nicht mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung muss ein eigenes, eigenständiges Passwort verwendet werden.
- 3. Verbot schwacher oder häufig genutzter Passwörter:** Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten auftauchen, dürfen nicht verwendet werden.
- 4. Geheimhaltung der Passwörter:** Passwörter müssen geheim gehalten werden. Sie dürfen nur persönlich bekannt sein und müssen unbeobachtet eingegeben werden.
- 5. Verbot der Speicherung auf Hardware-Funktionstasten:** Passwörter dürfen nicht auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden.
Schriftliche Fixierung nur im Notfall: Ein Passwort darf nur für eine Hinterlegung im Notfall schriftlich fixiert werden – aber muss sicher aufbewahrt werden.
- 6. Empfehlung eines Passwort-Managers:** Der Einsatz eines Passwort-Managers sollte geprüft werden.

- 7. Passwortwechsel bei Verdacht auf Kompromittierung:** Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt wurde oder auch nur der Verdacht darauf besteht.

7 Änderungshistorie

VERSION	STAND	BEARBEITER	ÄNDERUNGEN / KOMMENTARE
1.0	30.08.2024	Anna Lena Schwerdtfeger	Ersterstellung
1.1	09.10.2024	Anna Lena Schwerdtfeger	Hinzufügen von Bildern
2.0	01.09.2025	Jessica Zorn	Umfassende inhaltliche Überarbeitung
2.1	14.01.2026	Anna Lena Schwerdtfeger	Inhaltliche Überprüfung und Formatanpassungen
2.2	22.01.2026	Anna Lena Schwerdtfeger	Anpassung von Bildern