NO GLYPH

Videokonferenz

Superadmin-Handbuch

VERTRAULICH

SUPERADMIN · HANDBUCH

Version 1.0 · April 2026

Inhaltsverzeichnis

1 Einführung – Die Superadmin-Rolle 3

2 Anmelden unter /admin 3

3 Raumverwaltung 4

4 Benutzerverwaltung 6

5 Konfiguration (SMTP) 8

6 Medienverwaltung 9

7 Sicherheitshinweise 9

1 Einführung – Die Superadmin-Rolle

Der **Superadmin** hat die vollständige Kontrolle über das Videokonferenz-System. Im Gegensatz zu Moderatoren wird der Superadmin-Zugang nicht über die normale Benutzerverwaltung, sondern direkt über Umgebungsvariablen in der Server-Konfigurationsdatei (`.env`) eingerichtet.

Vollständige Raumverwaltung

Alle Räume anlegen, bearbeiten, löschen und konfigurieren – unabhängig vom Eigentümer.

Benutzerverwaltung

Benutzerkonten einsehen, Status ändern, Rollen vergeben, Berechtigungen setzen.

⚙

Systemkonfiguration

SMTP-Einstellungen für E-Mail-Versand, globale Systemparameter verwalten.

Medienverwaltung

MP3-Dateien und Videos für Räume hochladen und verwalten.

Superadmin-Rechte schützen

Der Superadmin hat uneingeschränkten Zugriff auf alle Systemdaten. Geben Sie Zugangsdaten niemals weiter. Verwenden Sie ausschließlich starke, einzigartige Passwörter. Dieses Handbuch ist als vertraulich zu behandeln.

2 Anmelden unter /admin

Das Admin-Panel ist unter einer separaten URL erreichbar: `/admin`. Die Zugangsdaten werden **nicht** über die normale Benutzerdatenbank verwaltet, sondern sind fest in der Server-Konfiguration hinterlegt.

2.1 Zugangsdaten konfigurieren (.env)

Die Superadmin-Zugangsdaten werden in der Datei `.env` auf dem Server definiert. Relevante Variablen:

```
# Superadmin-Zugangsdaten
ADMIN_USERNAME=admin
ADMIN_PASSWORD=IhrSicheresPasswort123!

# LiveKit-Konfiguration
LIVEKIT_URL=wss://livekit.beispiel.de
LIVEKIT_API_KEY=IhrApiKey
LIVEKIT_API_SECRET=IhrApiSecret

# Datenbank
DATABASE_URL=postgresql://user:pass@localhost/videokonferenz
```

.env-Datei niemals veröffentlichen

Die `.env`-Datei enthält alle sensiblen Zugangsdaten. Sie darf niemals in ein Versionskontrollsystem (Git) eingecheckt oder öffentlich zugänglich sein. Stellen Sie sicher, dass `.env` in der `.gitignore` eingetragen ist.

2.2 Anmeldeprozess

1 Admin-URL aufrufen

Öffnen Sie in Ihrem Browser die Adresse `https://ihre-domain.de/admin`. Sie werden zur Admin-Anmeldeseite weitergeleitet.

2 Zugangsdaten eingeben

Geben Sie den in `.env` definierten **ADMIN_USERNAME** und das **ADMIN_PASSWORD** ein. Diese Zugangsdaten sind unabhängig von der normalen Benutzerdatenbank.

3 Admin-Dashboard öffnet sich

Nach erfolgreicher Anmeldung sehen Sie das Admin-Dashboard mit Navigation zu Raumverwaltung, Benutzerverwaltung, Konfiguration und Medien.

⚠ Separate Sitzung vom Moderator-Login

Der Admin-Login unter `/admin` ist vollständig getrennt vom Moderator-Login auf der Startseite. Sie können gleichzeitig als Superadmin unter `/admin` und als Moderator auf der Startseite angemeldet sein (in verschiedenen Browser-Tabs).

3 Raumverwaltung

Die Raumverwaltung ermöglicht Ihnen die vollständige Kontrolle über alle Konferenzräume im System. Sie finden sie im Admin-Dashboard unter dem Menüpunkt **„Räume"**.

3.1 Räume anlegen

1. **„Neuen Raum anlegen" klicken**
   Klicken Sie auf den Button „+ Neuen Raum anlegen". Das Raum-Formular öffnet sich.

2. **Pflichtfelder ausfüllen**
   Geben Sie **Name** (sichtbar für Teilnehmer), **Beschreibung** (optional), **Passwort** (optional) und den **Eigentümer** (Moderator-Account) ein.

3. **Funktionen aktivieren/deaktivieren**
   Wählen Sie, welche Funktionen in diesem Raum verfügbar sind (siehe 3.2). Diese Einstellungen können jederzeit geändert werden.

4. **Speichern**
   Klicken Sie auf „Speichern". Der Raum wird angelegt und dem angegebenen Moderator zugewiesen.

3.2 Raumfunktionen konfigurieren

Folgende Funktionen lassen sich pro Raum individuell ein- oder ausschalten:

Symbol	Funktion	Beschreibung & Auswirkung
	Musik-Player	Zeigt im Raum einen Musik-Player in der Seitenleiste an. Moderatoren können hochgeladene MP3-Dateien für alle Teilnehmer synchron abspielen.
	Video-Wiedergabe	Aktiviert den Video-Player. Moderatoren können Videos synchron für alle Teilnehmer abspielen und steuern.
	Bildschirm teilen	Erlaubt allen Teilnehmern und Moderatoren, ihren Bildschirm oder ein Fenster zu teilen. Wenn deaktiviert, ist der Button nicht sichtbar.
	Chat	Aktiviert den Text-Chat in der Seitenleiste. Alle Teilnehmer können Nachrichten schreiben und lesen. Wenn deaktiviert, gibt es keinen Chat-Tab.

3.3 Passwortschutz

Räume können optional mit einem Passwort gesichert werden. Teilnehmer müssen das Passwort eingeben, um beizutreten.

i Passwort zurücksetzen
Um das Passwort eines Raums zu entfernen, bearbeiten Sie den Raum und lassen das Passwortfeld leer. Bestehende Moderatoren werden nicht automatisch über Passwortänderungen informiert.

3.4 Räume bearbeiten und löschen

In der Raumliste sehen Sie alle Räume im System. Über die Aktionsspalte können Sie:

- ✏ **Bearbeiten:** Alle Raumeigenschaften und Funktionen anpassen.
- 🗑 **Löschen:** Raum unwiderruflich entfernen. Ein Bestätigungsdialog erscheint. Laufende Konferenzen werden sofort beendet.
- **Eigentümer ändern:** Den zugewiesenen Moderator wechseln.

4 Benutzerverwaltung

Die Benutzerverwaltung finden Sie im Admin-Dashboard unter **„Benutzer"**. Hier sehen Sie alle registrierten Benutzer mit ihren aktuellen Status, Rollen und Berechtigungen.

4.1 Benutzer-Status verstehen

Jeder Benutzer durchläuft einen Status-Lebenszyklus. Als Superadmin können Sie den Status jederzeit manuell setzen:

Status	Bedeutung & Fähigkeiten	Kann sich anmelden?
neu	Gerade registriert, E-Mail noch nicht bestätigt. Kein Zugriff auf Moderatorfunktionen.	Nein
✉ email_bestätigt	E-Mail-Adresse verifiziert. Wartet auf Admin-Freischaltung. Kein Login möglich.	Nein
moderator	Vollständig freigeschaltet. Kann sich anmelden und Moderatorfunktionen nutzen (gemäß Berechtigungen).	Ja
gesperrt	Account gesperrt. Kein Login möglich. Konfiguration und Räume bleiben erhalten.	Nein

4.2 Status eines Benutzers ändern

1. **Benutzer in der Liste finden**
   Nutzen Sie die Suchfunktion oben, um nach Name, Benutzername oder E-Mail zu filtern.
2. **Benutzer bearbeiten**
   Klicken Sie auf das Bearbeiten-Symbol (✏) oder auf den Benutzernamen, um das Benutzer-Bearbeitungsformular zu öffnen.
3. **Status auswählen**
   Wählen Sie im Dropdown-Menü „Status" den gewünschten Wert: neu, email_bestätigt, moderator oder gesperrt.
4. **Speichern**
   Klicken Sie auf „Speichern". Die Änderung wird sofort wirksam. Ein Benutzer mit Status gesperrt wird bei der nächsten Aktion automatisch ausgeloggt.

4.3 Rollen setzen

Neben dem Status gibt es zwei Rollen, die pro Benutzer gesetzt werden können:

Rolle	Beschreibung
user	Standardrolle für alle Moderatoren. Zugriff auf Moderatorfunktionen gemäß vergebener Berechtigungen.
superadmin	Erweiterte Rolle. Benutzer kann ebenfalls auf `/admin` zugreifen (wenn separat konfiguriert). Verwenden Sie diese Rolle mit äußerster Vorsicht.

4.4 Berechtigungen vergeben

Berechtigungen steuern, was ein Moderator unter `/mod` tun kann. Sie können einem Benutzer folgende Berechtigungen einzeln zuweisen:

create_rooms | manage_own_rooms | manage_all_rooms

Berechtigung	Was wird erlaubt?
`create_rooms`	Neuen Räume unter `/mod` anlegen. Ohne diese Berechtigung ist der „+ Neuer Raum"-Button nicht sichtbar.
`manage_own_rooms`	Eigene, zugewiesene Räume bearbeiten und löschen. Grundberechtigung für Moderatoren.
`manage_all_rooms`	Alle Räume im System verwalten – unabhängig vom Eigentümer. Erweiterte Berechtigung für leitende Moderatoren.

4.5 Räume einem Benutzer zuweisen

In der Benutzerbearbeitung können Sie Räume direkt einem Moderator zuweisen. Der Moderator sieht diese Räume dann in seiner Raumverwaltung unter `/mod`. Sie können mehrere Räume pro Benutzer zuweisen.

4.6 Passwort eines Benutzers zurücksetzen

Im Benutzer-Bearbeitungsformular finden Sie ein Feld **„Neues Passwort"**. Geben Sie ein neues Passwort ein und speichern Sie. Das alte Passwort wird sofort ungültig. Informieren Sie den Benutzer über das neue Passwort auf einem sicheren Weg.

> **⚠ Passwörter sicher übermitteln**
> Übermitteln Sie zurückgesetzte Passwörter niemals per unverschlüsselter E-Mail. Nutzen Sie verschlüsselte Kommunikationskanäle oder teilen Sie das Passwort persönlich mit.

5 Konfiguration

Unter dem Menüpunkt **„Konfiguration"** im Admin-Dashboard können Sie systemweite Einstellungen vornehmen. Der wichtigste Bereich ist die SMTP-Konfiguration für den automatischen E-Mail-Versand.

5.1 SMTP-Einstellungen für Aktivierungs-E-Mails

Damit Benutzer nach der Registrierung eine Bestätigungs-E-Mail erhalten, müssen SMTP-Daten konfiguriert sein. Diese Einstellungen können sowohl in der `.env`-Datei als auch über das Admin-Interface gepflegt werden.

```
# SMTP-Konfiguration für E-Mail-Versand
SMTP_HOST=smtp.beispiel.de
SMTP_PORT=587
SMTP_SECURE=false  # true für Port 465 (SSL)
SMTP_USER=noreply@beispiel.de
SMTP_PASS=IhrSMTPPasswort
SMTP_FROM="Videokonferenz <noreply@beispiel.de>"
```

Parameter	Beschreibung	Beispielwert
`SMTP_HOST`	Hostname des SMTP-Servers Ihres Mail-Providers	`smtp.gmail.com`
`SMTP_PORT`	Port des SMTP-Servers (587 für STARTTLS, 465 für SSL)	`587`
`SMTP_SECURE`	SSL/TLS: `true` für Port 465, `false` für STARTTLS	`false`
`SMTP_USER`	Benutzername/E-Mail-Adresse für die SMTP-Authentifizierung	`noreply@domain.de`
`SMTP_PASS`	Passwort für das SMTP-Konto	—
`SMTP_FROM`	Absendername und -adresse, die in E-Mails erscheint	`"System <noreply@...>"`

5.2 E-Mail-Konfiguration testen

Nutzen Sie im Admin-Interface den Button **„Test-E-Mail senden"**, um die SMTP-Konfiguration zu überprüfen. Nach dem Klick geben Sie eine Empfänger-Adresse ein und bestätigen. Wenn die E-Mail ankommt, ist die Konfiguration korrekt.

> **E-Mail-Dienste für Tests**
>
> Zum Testen empfiehlt sich ein Dienst wie **Mailtrap** oder **Mailhog** (Entwicklungsumgebung), der E-Mails abfängt ohne sie zu versenden. Für Produktion: Gmail App-Passwort, Mailgun, SendGrid oder eigener Mailserver.

6 Medienverwaltung

Unter dem Menüpunkt **„Medien"** verwalten Sie die Audiodateien und Videos, die in Konferenzräumen abgespielt werden können.

6.1 MP3-Dateien hochladen und verwalten

1 Raum auswählen

Wählen Sie aus dem Dropdown-Menü den Raum, für den Sie Musik-Dateien hinterlegen möchten. Jeder Raum hat eine eigene Medienbibliothek.

2 Datei hochladen

Klicken Sie auf „+ MP3 hochladen" und wählen Sie eine `.mp3`-Datei von Ihrem Computer. Die Datei wird auf den Server übertragen.

3 Metadaten eingeben (optional)

Geben Sie Titel, Künstler und Album ein, falls nicht automatisch aus der ID3-Tag erkannt. Diese Informationen werden im Musik-Player angezeigt.

6.2 Videos hochladen und verwalten

Das Verfahren ist identisch zum MP3-Upload. Unterstützte Videoformate sind üblicherweise `.mp4` und `.webm`. Achten Sie auf die Dateigröße – große Videos können den Upload verlangsamen.

⚠ Hinweis zu Dateigrößen

Je nach Server-Konfiguration gibt es eine maximale Upload-Größe. Diese kann in der `.env`-Datei über die Variable `MAX_UPLOAD_SIZE` angepasst werden (Angabe in Megabyte). Standard ist oft 50 MB.

6.3 Medien löschen

In der Medienliste klicken Sie auf 🗑 neben der Datei. Die Datei wird sofort vom Server gelöscht. Wenn die Datei gerade in einem laufenden Raum abgespielt wird, kann die Wiedergabe abbrechen.

7 Sicherheitshinweise

Dieses Kapitel ist besonders wichtig

Der Schutz des Videokonferenz-System liegt in Ihrer Verantwortung als Superadmin. Befolgen Sie alle folgenden Hinweise sorgfältig.

.env-Datei schützen

Setzen Sie restriktive Dateiberechtigungen: `chmod 600 .env`. Nur der Prozessbenutzer des Servers darf lesen. Niemals in Git einschecken – stellen Sie sicher, dass `.env` in der `.gitignore` steht.

Starkes Superadmin-Passwort verwenden

Mindestens 16 Zeichen, Kombination aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen. Verwenden Sie einen Passwort-Manager. Ändern Sie das Passwort regelmäßig (mindestens alle 90 Tage).

Admin-Zugang einschränken

Schränken Sie den Zugriff auf `/admin` per IP-Whitelist oder VPN ein, falls Ihr Webserver das unterstützt. Öffentlicher Internetzugang zum Admin-Panel ist ein Sicherheitsrisiko.

HTTPS verwenden

Betreiben Sie die Anwendung ausschließlich über HTTPS (TLS). Unverschlüsselte HTTP-Verbindungen ermöglichen das Abfangen von Passwörtern und Sitzungsdaten. Verwenden Sie Let's Encrypt für kostenlose TLS-Zertifikate.

Superadmin-Rolle sparsam vergeben

Setzen Sie die Rolle superadmin für Benutzeraccounts nur dann, wenn unbedingt erforderlich. Bevorzugen Sie granulare Berechtigungen (`manage_all_rooms` etc.) gegenüber vollständigen Admin-Rechten.

Regelmäßige Datensicherung

Führen Sie regelmäßige Backups der Datenbank und der hochgeladenen Medien durch. Testen Sie die Wiederherstellung der Backups regelmäßig.

Server-Logs überwachen

Überwachen Sie die Server-Logs auf verdächtige Aktivitäten, insbesondere wiederholt fehlgeschlagene Anmeldeversuche am Admin-Panel (Brute-Force-Angriffe). Erwägen Sie Rate-Limiting auf Login-Endpunkten.

Software aktuell halten

Aktualisieren Sie die Anwendung und alle Abhängigkeiten (Node.js-Pakete, LiveKit-Server, Betriebssystem) regelmäßig, um bekannte Sicherheitslücken zu schließen.

Immer abmelden

Melden Sie sich nach der Arbeit im Admin-Panel immer ab. Lassen Sie keine Admin-Sitzungen unbeaufsichtigt offen. Konfigurieren Sie kurze Sitzungstimeouts.

Sicherheitsvorfall melden

Bei Verdacht auf einen Sicherheitsvorfall (unbefugter Zugriff, Datenverlust, verdächtige Aktivitäten): Ändern Sie sofort alle Passwörter, sperren Sie betroffene Accounts und sichern Sie die aktuellen Logs. Informieren Sie alle betroffenen Benutzer gemäß Datenschutzgrundverordnung (DSGVO).