

Gitea

Anleitung

<https://docs.gitea.com/installation/install-with-docker>

<https://integrations.goauthentik.io/integrations/services/gitea/>

<https://docs.gitea.com/administration/config-cheat-sheet>

Runner:

<https://docs.gitea.com/usage/actions/act-runner#install-with-the-docker-image>

<https://docs.gitea.com/usage/actions/act-runner#configuration>

docker-compose.yml mit Runner

update mit v1.25.4 am 03.02.2026

```
services:
  server:
    image: docker.gitea.com/gitea:1.25.4
    container_name: gitea
    environment:
      - USER_UID=1000
      - USER_GID=1000
      - GITEA__database__DB_TYPE=postgres
      - GITEA__database__HOST=db:5432
      - GITEA__database__NAME=gitea
      - GITEA__database__USER=gitea
      - GITEA__database__PASSWD=<openssl rand -hex 24>
    restart: always
```

```
networks:
  - gitea
volumes:
  - app:/data
  - /etc/timezone:/etc/timezone:ro
  - /etc/localtime:/etc/localtime:ro
ports:
  - "3046:3000"
  - "222:22"
depends_on:
  - db
```

```
db:
  image: docker.io/library/postgres:14
  restart: unless-stopped
  environment:
    - POSTGRES_USER=gitea
    - POSTGRES_PASSWORD=<openssl rand -hex 24>
    - POSTGRES_DB=gitea
  networks:
    - gitea
  volumes:
    - db:/var/lib/postgresql/data
```

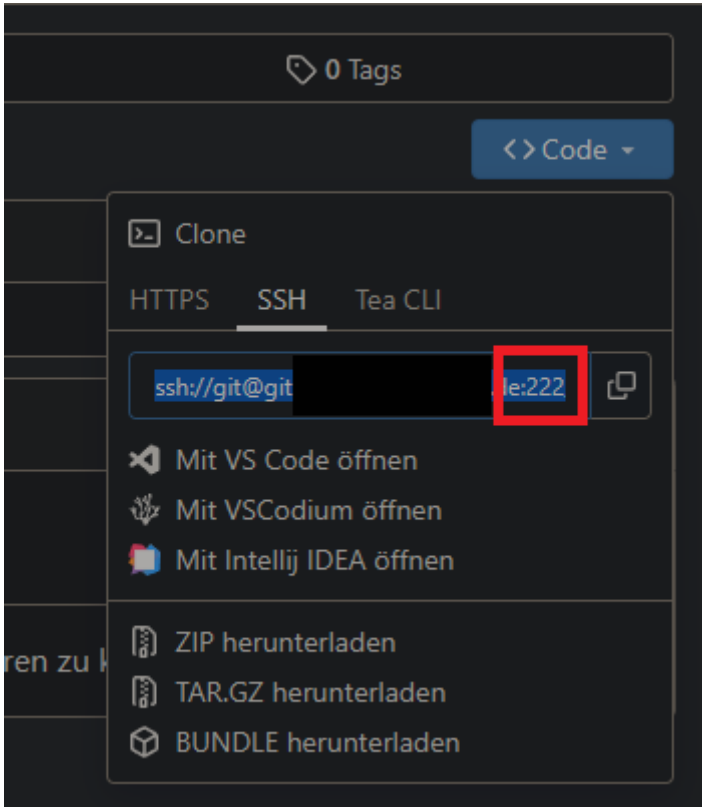
```
runner:
  image: docker.io/gitea/act_runner:0.2.13
  environment:
    CONFIG_FILE: /config.yaml
    GITEA_INSTANCE_URL: "https://git.MEINEDOMAIN.DE"
    GITEA_RUNNER_REGISTRATION_TOKEN: "r5ES....ptLTD" # Token aus gitea web-ui Einstellungen
```

> Actions > Runner > create Runner

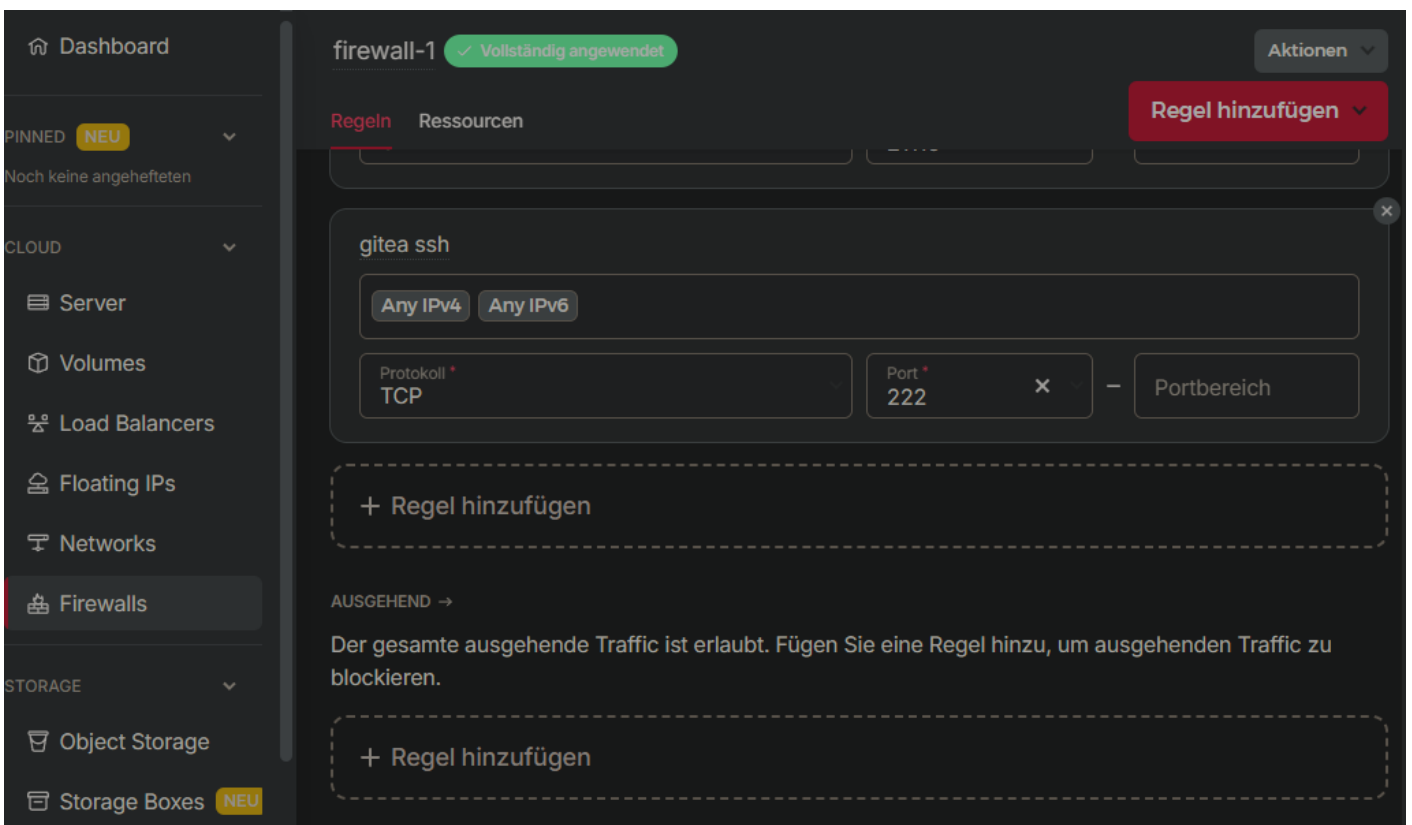
```
GITEA_RUNNER_NAME: "gitea-runner-01"
GITEA_RUNNER_LABELS: "ubuntu-22.04:host"
volumes:
  - /mnt/fn-volume-01/docker-data/volumes/gitea_runner-cfg/config.yaml:/config.yaml
  - runner-data:/data
  - /var/run/docker.sock:/var/run/docker.sock
```

```
networks:
```


Danach den Gitea-Container neustarten und in einem Repo unter Code > SSH die Adresse checken, ob der Port übernommen wurde:

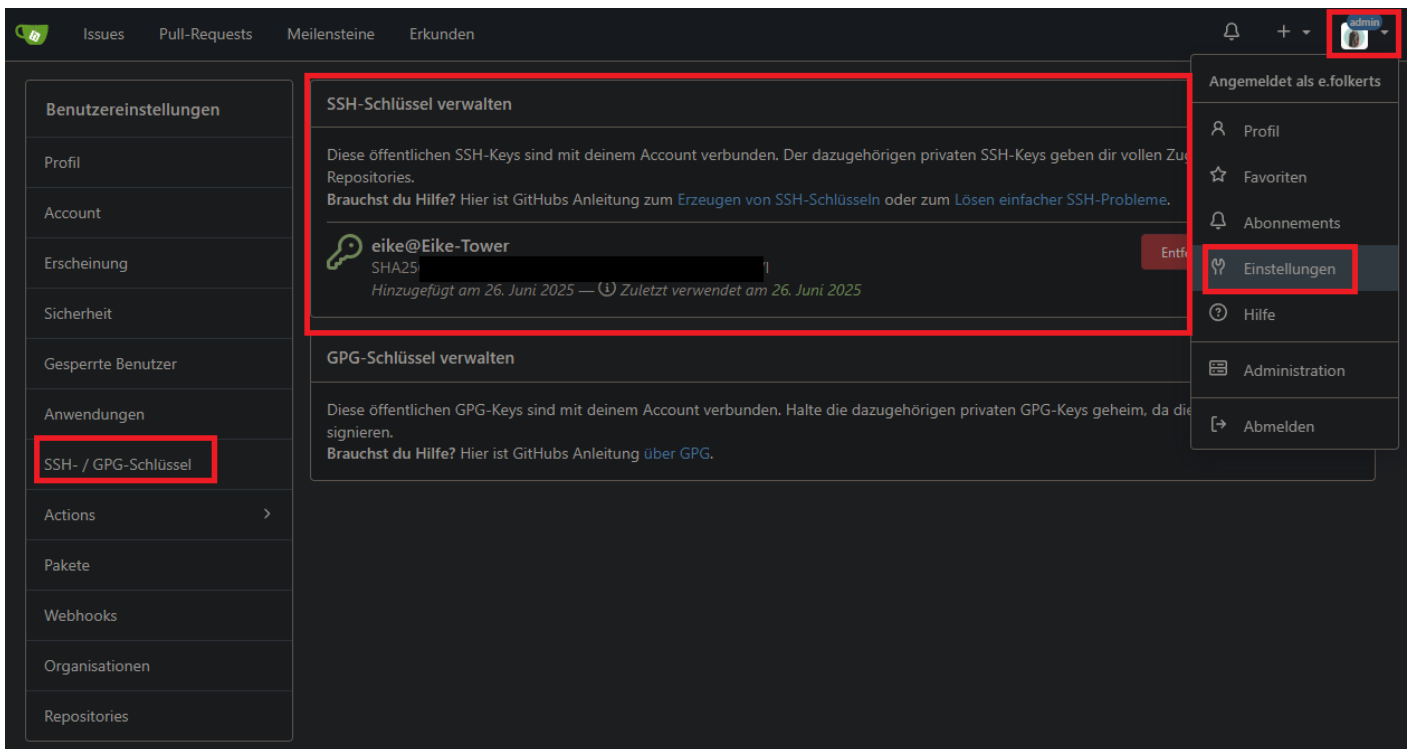


Nicht vergessen, den Port in der Firewall zu öffnen, in meinem Fall Hetzner, ansonsten auch in der ufw



Um den eigenen SSH-Key verwenden zu können, muss der Public-Key natürlich noch in Gitea eingepflegt werden unter

Profilbild > Einstellungen > SSH / GPG-Schlüssel > Schlüssel hinzufügen > .pub-Key einfügen und benennen



ssh testen mit

```
ssh -p 222 -i /home/BENUTZER/.ssh/id_MEINNAME_ed25519 git@git.DEINEDOMAIN.de
```

wenn successfully authenticated, testen mit git clone:

```
~/gitea-pl > ls
~/gitea-pl > git clone ssh://git@git.[REDACTED]:222/[REDACTED]/ansible.git
Cloning into 'ansible'...
The authenticity of host '[REDACTED]:222 ([49.13.52.176]:222)' can't be established.
ECDSA key fingerprint is SHA256:[REDACTED].
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[REDACTED]:222,[REDACTED]:222' (ECDSA) to the list of known hosts.
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 6 (delta 1), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (6/6), done.
Resolving deltas: 100% (1/1), done.
~/gitea-pl > ls
ansible
~/gitea-pl > |
```

Falls ein anderer ssh-key angegeben werden muss, kann dies in der ~/.ssh/config eingestellt werden (Datei anlegen, falls nicht vorhanden):

```
~ > cat /home/eike/.ssh/config
```

```
Host git.MEINEDOMAIN.de
  HostName git.MEINEDOMAIN.de
  Port 222
  User git
  IdentityFile ~/.ssh/id_MEINNAME_ed25519
```

OIDC-Settings in Authentik

app.ini Configuration

<https://docs.gitea.com/administration/config-cheat-sheet>

nano /var/lib/docker/volumes/gitea_app/_data/gitea/conf/app.ini:

```
[service]
# ...
DISABLE_REGISTRATION = false
REQUIRE_SIGNIN_VIEW = true
ALLOW_ONLY_EXTERNAL_REGISTRATION = true
ENABLE_AUTO_REGISTRATION = true
# ...

[openid]
ENABLE_OPENID_SIGNIN = true
ENABLE_OPENID_SIGNUP = true

# ...
```

Anwendungen > Provider > gitea

Aktualisieren Sie den OAuth2-Provider



Name *

Autorisierungs-Flow *

Flow der zur Authorisierung des Provider verwendet wird.

▼ Protokolleinstellungen

Clienttyp *

Vertraulich

Vertrauliche Clients sind in der Lage, die Vertraulichkeit ihrer Anmeldedaten, beispielsweise des Client-Geheimnisses, zu wahren

Öffentlich

Öffentliche Clients können die Vertraulichkeit nicht gewährleisten und sollten Methoden wie PKCE nutzen.

Client ID *

Client Geheimnis

Redirect URIs/Origins

Strict



(RegEx) *

[+ Add entry](#)

Valid redirect URIs after a successful authorization flow. Also specify any origins here for Implicit flows.

Wenn keine expliziten Umleitungs-URLs angegeben sind, wird die erste erfolgreich verwendete Umleitungs-URL gespeichert.

To allow any redirect URI, set the mode to RegEx and the value to "*". Be aware of the possible security implications this can have.

Signatur Schlüssel

Schlüssel zum Signieren der Token.

Privater Schlüssel

Schlüssel, der zum Verschlüsseln der Tokens benutzt wird.

> Advanced flow settings

> Erweiterte Protokolleinstellungen

> Machine-to-Machine-Authentifizierungseinstellungen

Aktualisieren

Abbrechen

Aktualisieren Sie den OAuth2-Provider



Erweiterte Protokolleinstellungen

Gültigkeit des Zugangsschlüssels `minutes=1`
Konfigurieren Sie, wie lange Zugangsschlüssel gültig sind.
(Format: hours=1;minutes=2;seconds=3) . ?

Zugriffsschlüsselgültigkeit `minutes=5`
Konfigurieren Sie, wie lange Zugangstoken gültig sind.
(Format: hours=1;minutes=2;seconds=3) . ?

Refresh Token Gültigkeit `days=30`
Konfigurieren Sie, wie lange Refresh Token gültig sind.
(Format: hours=1;minutes=2;seconds=3) . ?

Umfang

Available Scopes	Selected Scopes
<input type="text" value=""/>	<input type="text" value=""/>
<ul style="list-style-type: none">authentik default OAuth Mapping: Proxy outpostauthentik default OAuth Mapping: OpenID 'email' ✓authentik default OAuth Mapping: Application Entitlementsgitea ✓authentik default OAuth Mapping: authentik API accessauthentik default OAuth Mapping: OpenID 'offline_access'olivetin_scopeauthentik default OAuth Mapping: OpenID 'openid' ✓Nextcloud Profileauthentik default OAuth Mapping: OpenID 'profile' ✓vikunja_scope	<p>4 item(s) selected.</p> <ul style="list-style-type: none">authentik default OAuth Mapping: OpenID 'email'authentik default OAuth Mapping: OpenID 'openid'authentik default OAuth Mapping: OpenID 'profile'gitea

Wählen Sie aus, welche Bereiche vom Client verwendet werden können. Der Client muss noch den Bereich für den Zugriff auf die Daten angeben.

Betreffmodus

- Basierend auf der gehashten ID des Benutzers
- Basierend auf der ID des Benutzers
- Basierend auf der UUID des Benutzers
- Basierend auf dem Nutzernamen des Benutzers
- Basierend auf der E-Mail Adresse des Benutzers
Dies wird gegenüber dem UPN-Modus empfohlen.
- Basierend auf der UPN des Benutzers
Erfordert, dass der Benutzer ein 'upn'-Attribut gesetzt hat, und greift auf die gehashte Benutzer-ID zurück. Verwenden Sie diesen Modus nur, wenn Sie unterschiedliche UPN- und Mail-Domänen haben.

Konfigurieren Sie, welche Daten als eindeutige Benutzererkennung verwendet werden sollen. In den meisten Fällen sollte die Standardeinstellung in Ordnung sein.

Aktualisieren **Abbrechen**

Anwendungen > Anwendungen > Gitea

Anwendung aktualisieren ×

Name *
Anzeigename der Applikation

Slug *
Internal application name used in URLs.

Gruppe
Geben Sie optional einen Gruppennamen ein. Anwendungen in gleicher Gruppe werden gruppiert angezeigt.

Schnittstellen
Wählen einen Anbieter aus, welchen diese Anwendung benutzen soll.

Backchannel Providers
Wähle einen Rückkanal Anbieter welcher der Funktionalität des Hauptanbieters entspricht-

Richtlinien-Engine-Modus *

- any
Beliebige Bedingung muss erfüllt sein, um Zugang gewährt zu bekommen.
- all
Alle Bedingungen müssen erfüllt sein, um Zugang gewährt zu bekommen.

▼ UI-Einstellungen

Start URL
Wenn diese Option leer bleibt, versucht Authentik, die Start-URL auf der Grundlage des ausgewählten Providers zu extrahieren.

Im neuen Tab öffnen
Wenn diese Option aktiviert ist, wird die Aufruf-URL in einer neuen Browser-Registerkarte oder einem neuen Fenster der Anwendungsbibliothek des Benutzers geöffnet.

Symbol Keine ausgewählt
Aktuell eingestellt auf: /media/public/application-icons/gitea.png

Symbol zurücksetzen
Lösche das aktuell festgelegte Symbol.

Herausgeber

Beschreibung

Customization > Eigenschaften > Scope Mapping

gitea scope für gruppen gituser, gitadmin und gitrestricted

Aktualisiere Scope Mapping



Name *

Bereichsname *

Gültigkeitsbereich, den der Client angeben kann, um auf diese Eigenschaften zuzugreifen.

Beschreibung

Beschreibung, die Benutzer sehen, wenn sie Einwilligen. Falls leer gelassen, werden Benutzer nicht informiert.

Ausdruck *

```
1 gitea_claims = {}
2
3 if request.user.ak_groups.filter(name="gituser").exists():
4     gitea_claims["gitea"] = "user"
5 if request.user.ak_groups.filter(name="gitadmin").exists():
6     gitea_claims["gitea"] = "admin"
7 if request.user.ak_groups.filter(name="gitrestricted").exists():
8     gitea_claims["gitea"] = "restricted"
9
10 return gitea_claims
```

Ausdruck mit Python. [Eine Liste aller Variablen finden Sie in der Dokumentation.](#)

Aktualisieren

Abbrechen

```
gitea_claims = {}

if request.user.ak_groups.filter(name="gituser").exists():
    gitea_claims["gitea"] = "user"
if request.user.ak_groups.filter(name="gitadmin").exists():
    gitea_claims["gitea"] = "admin"
if request.user.ak_groups.filter(name="gitrestricted").exists():
    gitea_claims["gitea"] = "restricted"

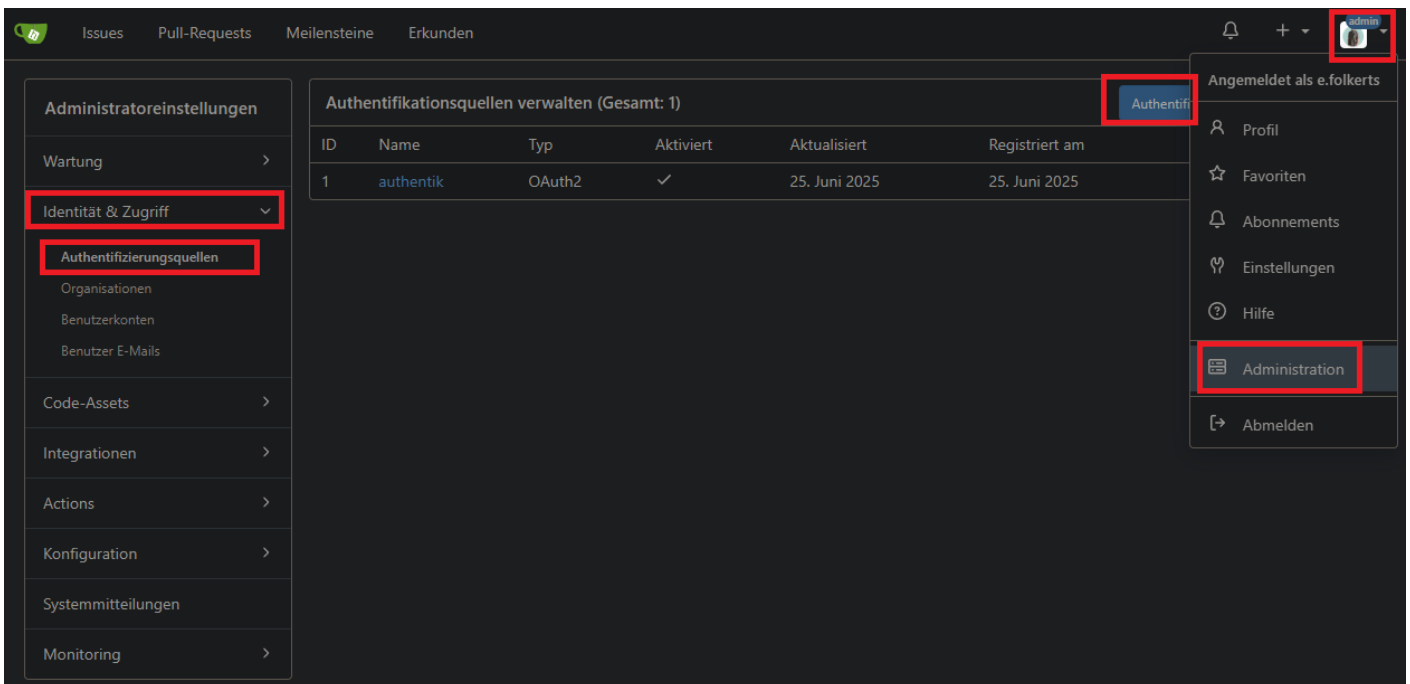
return gitea_claims
```

Verzeichnis > Gruppen



OIDC-Settings in Gitea

Administration > Identität & Zugriff > Authentifizierungsquellen > Neu:



- Administratoreinstellungen
- Wartung >
- Identität & Zugriff >
 - Authentifizierungsquellen
 - Organisationen
 - Benutzerkonten
 - Benutzer E-Mails
- Code-Assets >
- Integrationen >
- Actions >
- Konfiguration >
- Systemmitteilungen
- Monitoring >

Authentifikationsquelle bearbeiten

Authentifizierungstyp OAuth2

Authentifizierungsname *

Lokale 2FA überspringen
Leer lassen bedeutet, dass lokale User die 2FA immer noch bestehen müssen, um sich anzumelden

OAuth2-Anbieter *

Client-ID (Schlüssel) *

Client-Secret *

Symbol-URL

OpenID-Connect-Auto-Discovery-URL *

Zusätzliche Bereiche

Benötigter Claim-Name

Setze diesen Namen, damit Nutzer aus dieser Quelle sich nur anmelden dürfen, wenn sie einen Claim mit diesem Namen besitzen

Benötigter Claim-Wert

Setze diesen Wert, damit Nutzer aus dieser Quelle sich nur anmelden dürfen, wenn sie einen Claim mit diesem Namen und Wert besitzen

Claim-Name, der Gruppennamen für diese Quelle angibt. (Optional)

Gruppen-Claim Wert für Administratoren. (Optional - erfordert Claim-Namen oben)

Gruppen-Claim Wert für eingeschränkte User. (Optional - erfordert Claim-Namen oben)

Gruppen aus OAuth-Claims den Organisationsteams zuordnen. (Optional - oben muss der Name des Claims angegeben werden)

- Benutzer aus synchronisierten Teams entfernen, wenn der Benutzer nicht zur entsprechenden Gruppe gehört.
- Benutzersynchronisation aktivieren
- Diese Authentifikationsquelle ist aktiviert

Tipps

GMail Settings:
Host: smtp.gmail.com, Port: 587, Enable TLS Encryption: true

groß- und kleinbuchstaben beachten, alles so nennen wie in anleitung (auch scope, gruppen, claims, slug bei provider usw)

Revision #14

Created 2025-06-26 09:17:39 UTC

Updated 2026-02-05 10:33:08 UTC