Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kdo Cy / CEA
CoE Software Engineering

Richtlinie zum Ablauf von GitLab-Mitgliedschaften

Version 1.0.0-2-g24d61c2, 16.11.2026

Tabelle 1. Referenzen

Erkennungszeichen	Titel
EMBAG	https://www.fedlex.admin.ch/eli/cc/2023/682/de
BK «OSS Hilfsmittel»	https://www.bk.admin.ch/de/oss-hilfsmittel

Inhaltsverzeichnis

1. Zweck **3**
2. Policy **3**
3. Implementation **3**

1. Zweck

Dieses Vorgehen soll sicherstellen, dass ausschliesslich jene Personen auf GitLab-Projekte zugreifen, die aktiv und erforderlich eingebunden sind. Falls ein Account nicht mehr benötigt wird, verfällt sein Zugriff automatisch nach einer bestimmten Laufzeit. Damit wird der Aufwand für eine manuelle Nachverfolgung verringert.

2. Policy

Alle Mitgliedschaften in Untergruppen und Projekten (ausgenommen solche mit Access Level Owner) laufen nach einer definierten Zeit ab, unabhängig von der Aktivität. Eine Verlängerung erfolgt nur, indem der Project Owner die Mitgliedschaft neu erteilt. Die Laufzeit (validity) hängt vom Access Level ab und wird je nach Identifier-Typ zusätzlich durch einen Faktor beeinflusst. In der obersten Gruppe laufen Mitgliedschaften nicht ab.

Die Access Levels (mit ihren jeweiligen Grundlaufzeiten) lauten:

- No access: 10 Tage
- Minimal access: 20 Tage
- Guest: 90 Tage
- Reporter: 180 Tage
- Developer: 365 Tage
- Maintainer: 730 Tage
- Owner: Keine Ablaufzeit

Für identifizierte User wird die Grundlaufzeit mit dem gitlab_validity_factor des jeweiligen Identifier-Type multipliziert:

- U-Nummer (id=1): Faktor 1.5
- VBS (id=2): Faktor 0.2
- AHV (id=3): Faktor 0.2
- UL-Nummer (id=4): Faktor 0.2

Dadurch ergibt sich die tatsächliche Ablaufzeit als Grundlaufzeit (abhängig vom Access Level) multipliziert mit dem jeweiligen Faktor (abhängig vom Identifier-Type).

3. Implementation

1. In der obersten Gruppe (swiss-armed-forces) laufen Mitgliedschaften nicht ab, damit die SAML-Identität der User erhalten bleibt:
    - Alle abrechenbaren User werden als Guest hinzugefügt, falls sie noch nicht Mitglied sind.
    - Anschliessend erhalten alle User ausser Ownern den Access Level Minimal access. User mit einem höheren Access Level in einer Untergruppe oder einem Projekt erhalten Guest, damit sie den Dependency Proxy nutzen können.
2. In allen Untergruppen und Projekten wird für jede Mitgliedschaft das Ablaufdatum

berechnet: Erstellungsdatum der Mitgliedschaft plus Grundlaufzeit des Access Levels, multipliziert mit dem gitlab_validity_factor des Identifier-Typs. Die Aktivität spielt dabei keine Rolle.

3. Liegt das Ablaufdatum in der Zukunft, wird es in GitLab gesetzt; ist es erreicht, wird die Mitgliedschaft in der betreffenden Untergruppe oder dem Projekt entfernt.
4. Bots werden übersprungen. Bei Ownern wird ein allfälliges Ablaufdatum entfernt.
5. Eine Verlängerung erfolgt nur, indem der Project Owner die Mitgliedschaft neu erteilt.