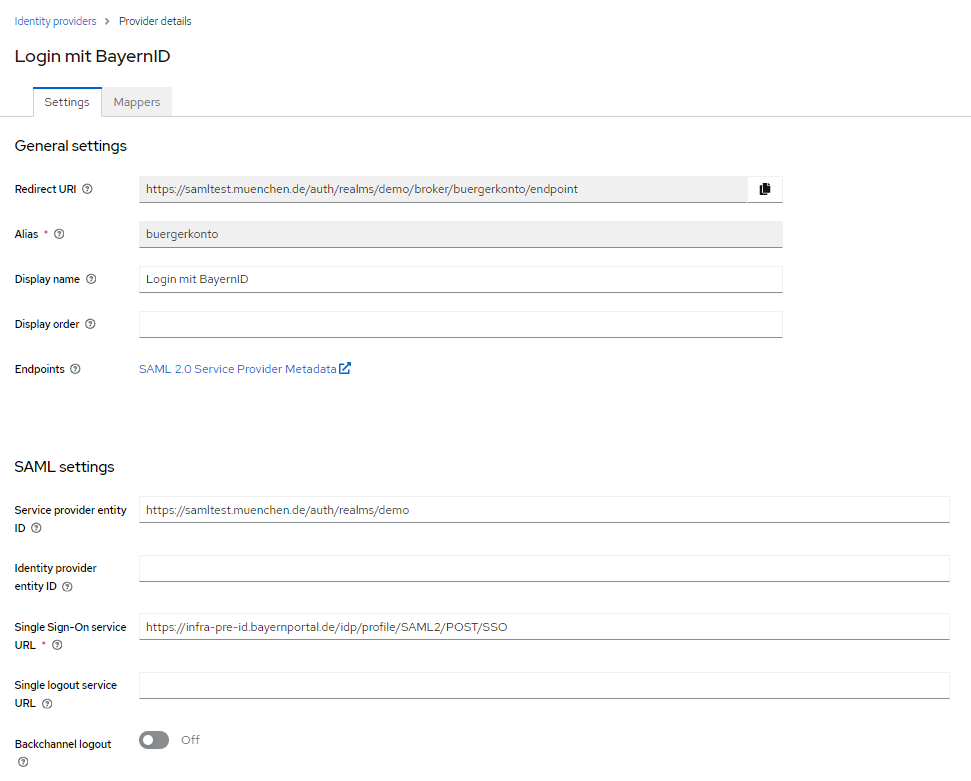
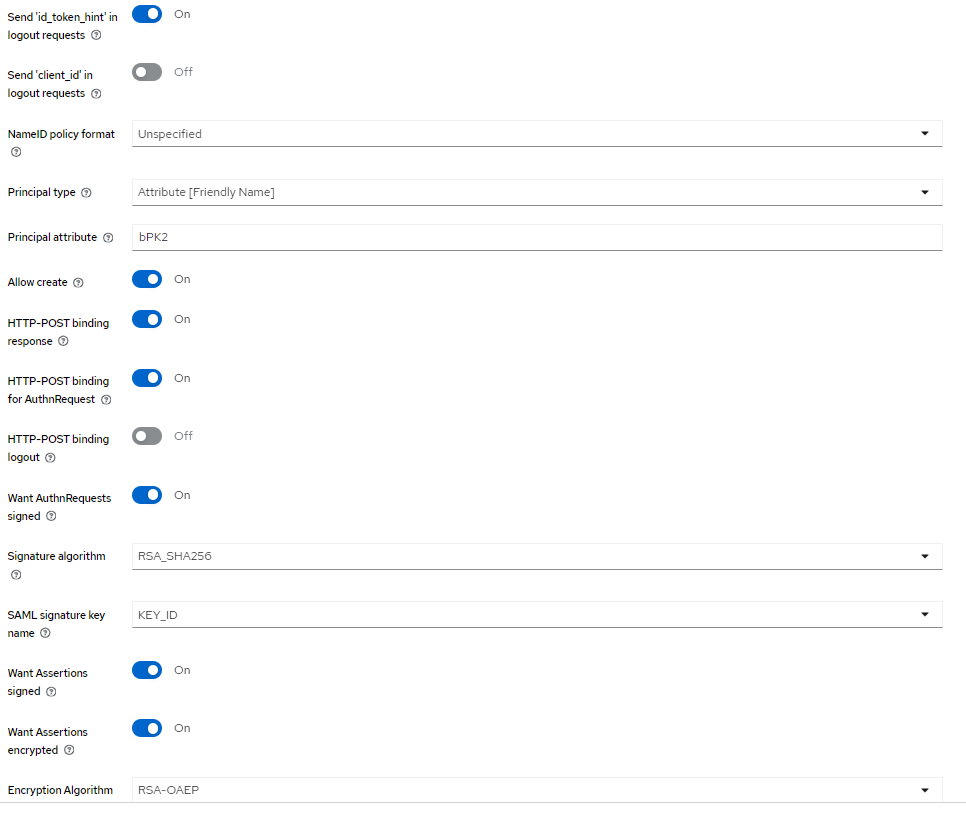
Konfiguration BayernID-Plugin

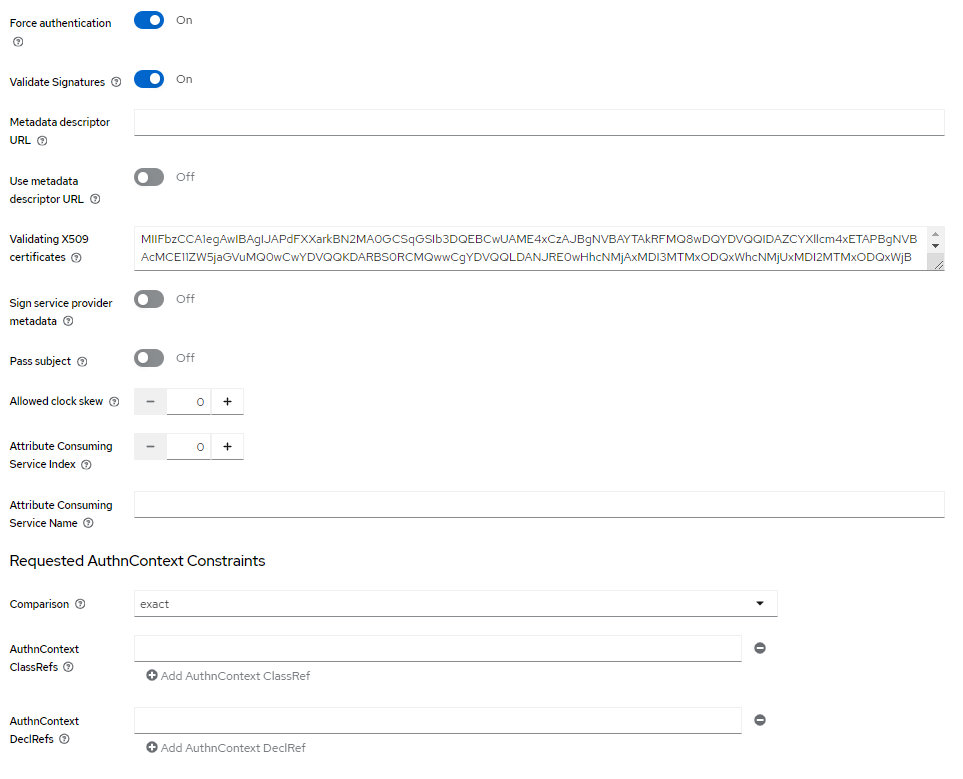
# SAML Konfig

Identity Providers → Add provider … → SAML v2.0



Konfig einspielen aus Metadata-Datei der AKDB, Herunterladen von hier: <https://infra-pre-id.bayernportal.de/idp>





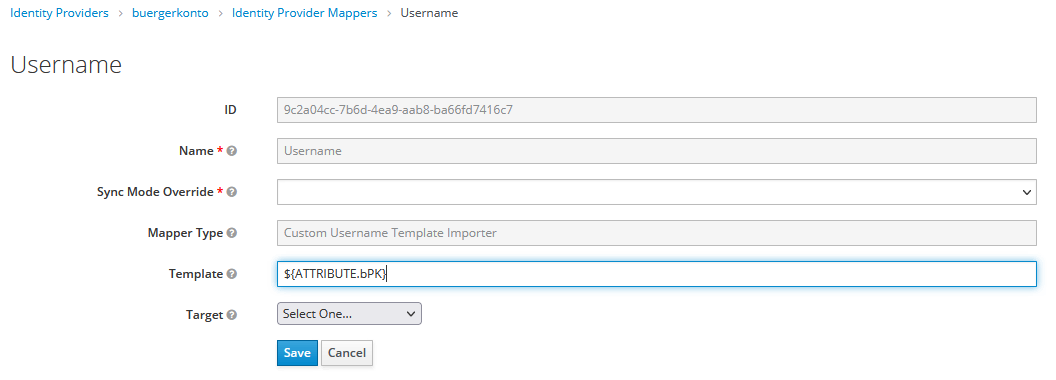
## Broker Mappers

Wichtig: Für Attribute den „CUSTOM Attribute-with-scope Mapper” verwenden, damit man die Attribute dann über die Scopes explizit im Request anfordern kann.

Username:

Name: username

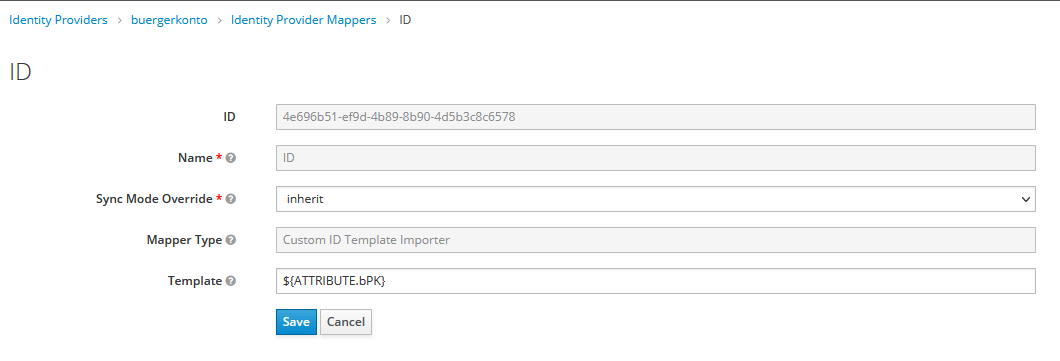
Template: ${ATTRIBUTE.bPK}



ID:

Name: ID

Template: ${ATTRIBUTE.bPK}



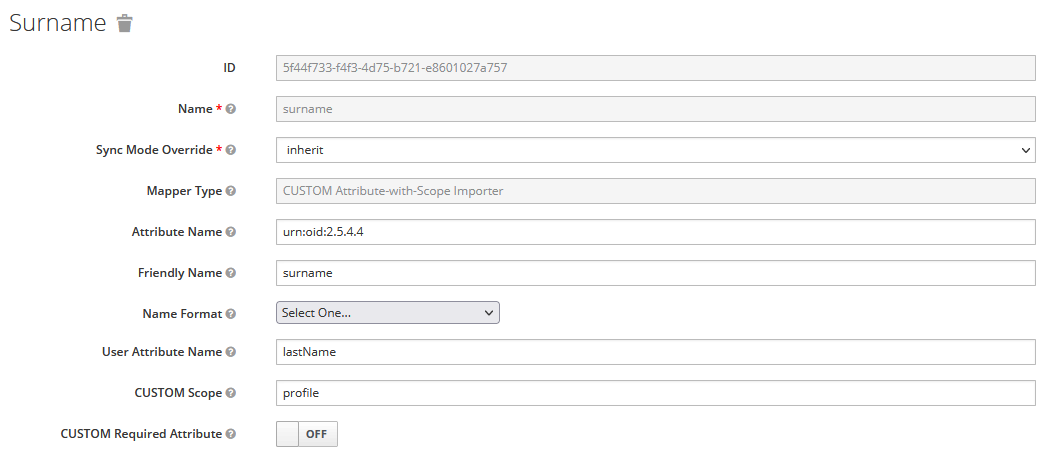
Surname:

Name: surname

Attribute Name: urn:oid:2.5.4.4

Friendly Name: surname

User Attribute Name: lastName



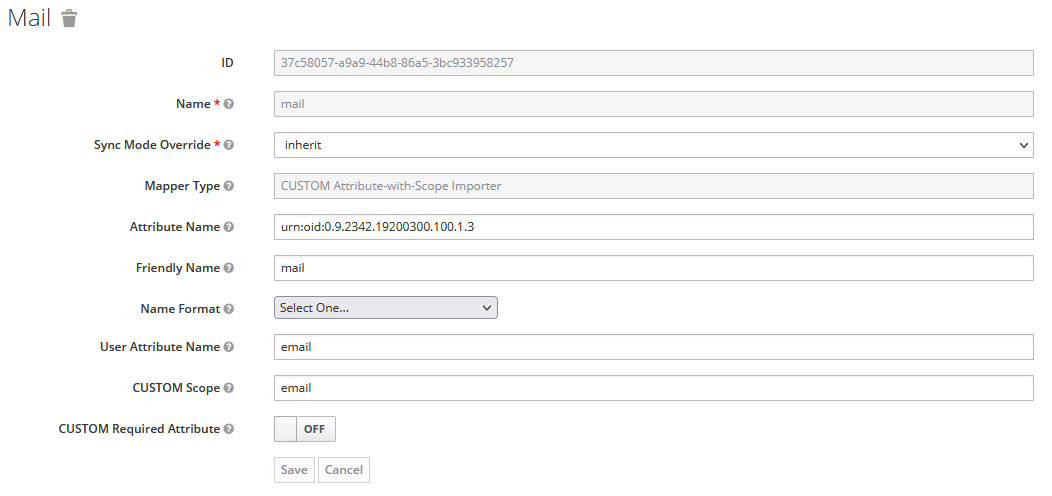
Mail:

Name: mail

Attribute Name: urn:oid:0.9.2342.19200300.100.1.3

Friendly Name: mail

User Attribute Name: email



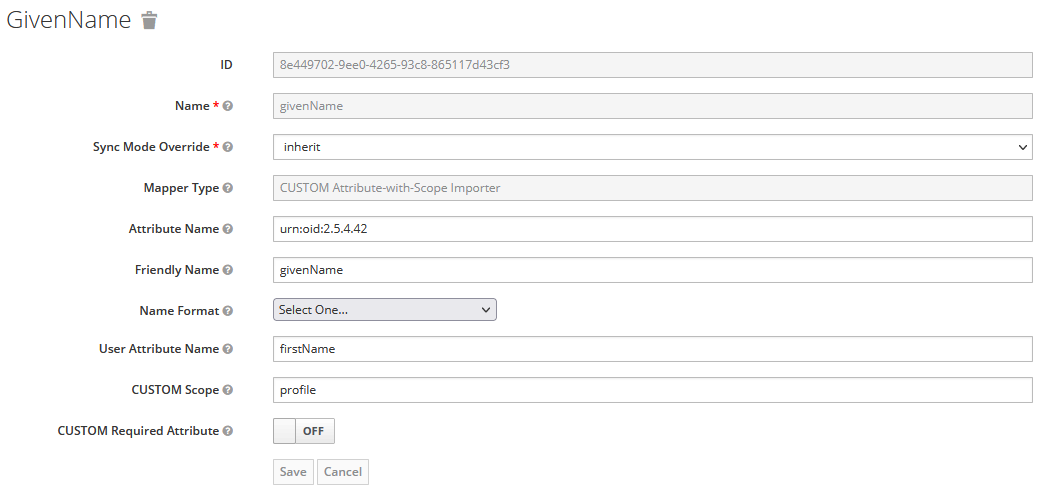
GivenName:

Name: givenName

Attribute Name: urn:oid:2.5.4.42

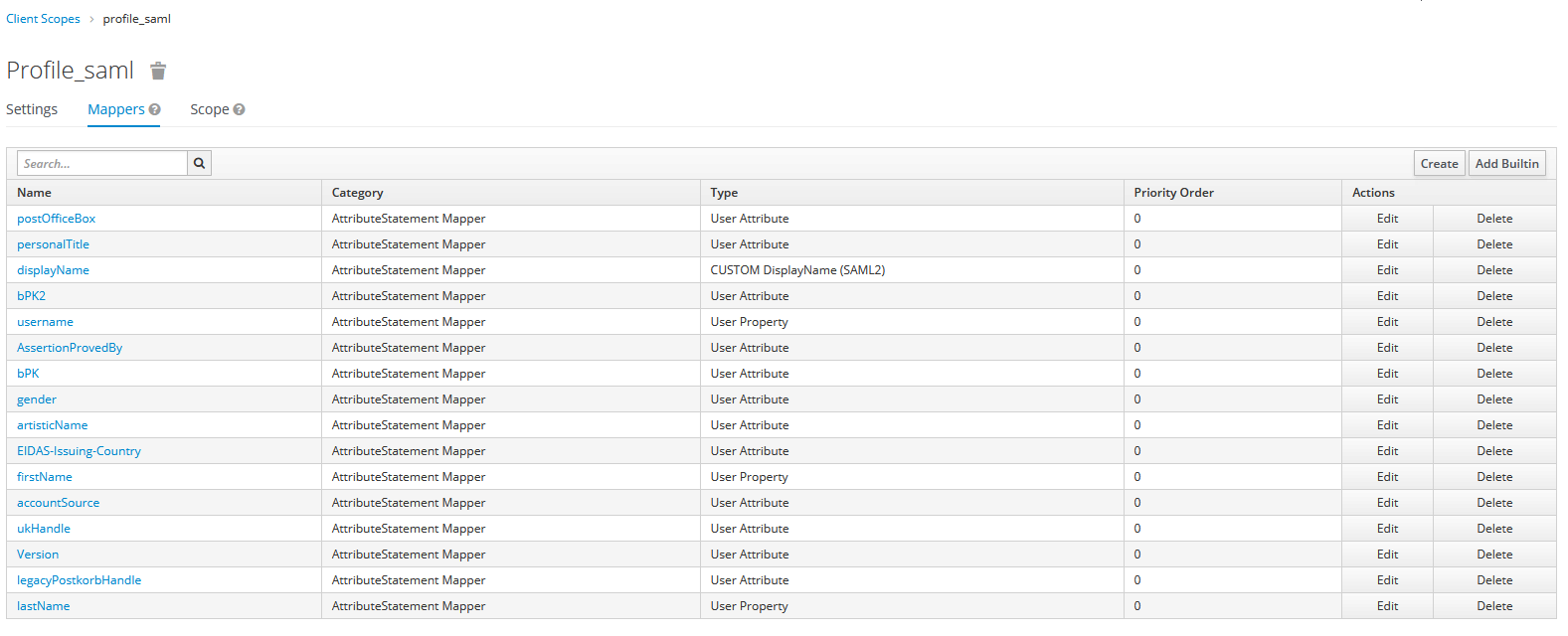
Friendly Name: givenName

User Attribute Name: firstName



usw. für alle anderen gewünschten Attribute (vgl. Doku der BayernID) – einen Export findet man in Datei **broker\_mappers.json** (kann man über Postman über die Keycloak-Admin-API einspielen).

In „CUSTOM Scope“ immer den Scope setzen, über den man das Attribut auch im Client ausspielen will, z.B. „Profile“. Um den gleichen Scope sowohl für OIDC als auch für SAML2 verwenden zu können, kann man die Suffixe „\_oidc“ und „\_saml“ verwenden, die bei der Verarbeitung aber vom Plugin vorher entfernt werden:



## Client Scopes definieren

Die Client Scopes sollte man so einrichten, dass alle Attribute der BayernID ausgeliefert werden können - sowohl für OIDC als auch für SAML2. Die Client Scopes sollten denen entsprechen, die man in den Broker Mappern konfiguriert hat.

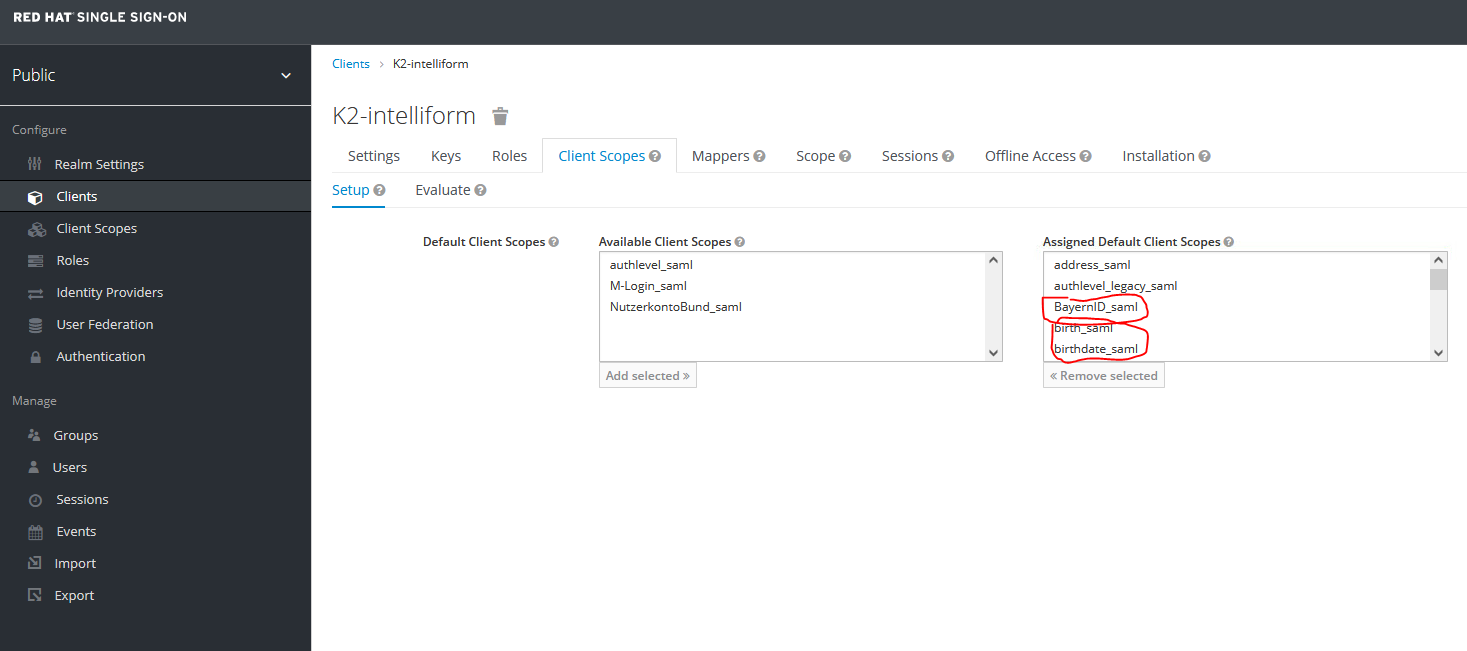
Außerdem sollte man folgende „Dummy-Scopes“ anlegen (jeweils für OIDC und für SAML2 mit Erweiterung „\_saml“):

* BayernID und BayernID\_saml
* level1 und level1\_saml
* level2 und level2\_saml
* level3 und level3\_saml
* level4 und level4\_saml
* debug

Eine vollständige Client Scope Konfiguration findet man in File **client\_scopes.json.**

## Client Scopes im Client konfigurieren

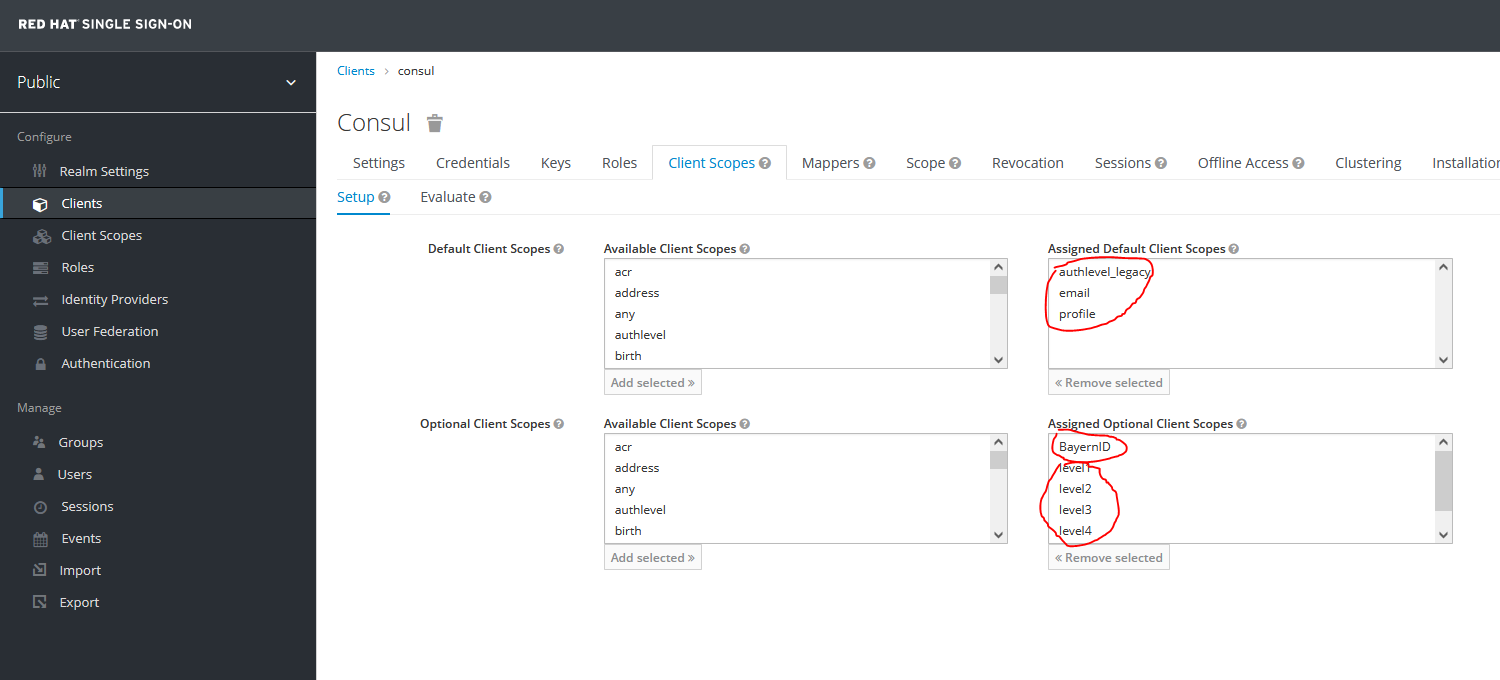
Im jeweiligen Client muss man die gewünschten Client Scopes dann explizit hinzufügen:



Es gibt zwei Typen von Client Scopes:

* „Echte“ Client Scopes (im Beispiel oben „birth\_saml“ und „birthdate\_saml“), die steuern
  + dass eine Menge von Attributen von der BayernID abgerufen werden (wenn im entsprechenden Broker-Mapper (s.o.) der gleiche Client Scope definiert wurde)
  + und diese Attribute auch im Client ausgeliefert werden
* Dummy Client Scopes, die steuern,
  + welche IDPs für den aktuellen Client aktiv sein sollen (im Beispiel oben die BayernID via „BayernID\_saml“)
  + welche Authlevel generell für diesen Client zugelassen sind (z.B. „level3“, wobei dies immer „mindestens“ bedeutet)

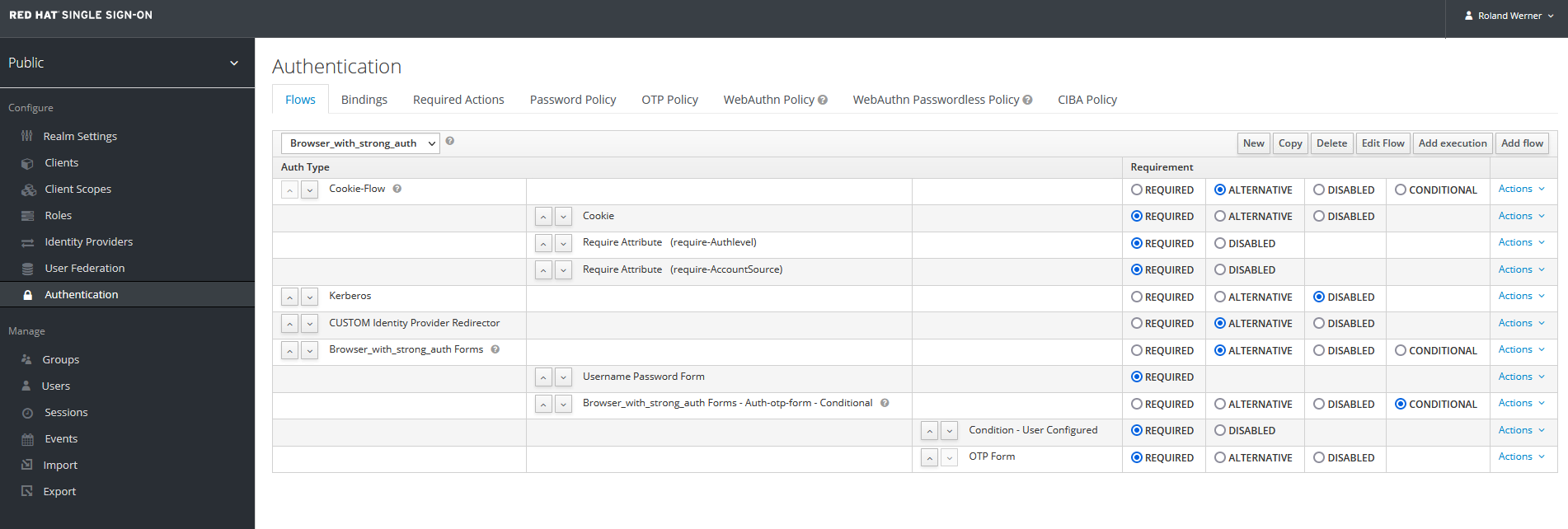
Bei OIDC sieht das etwas anders aus:

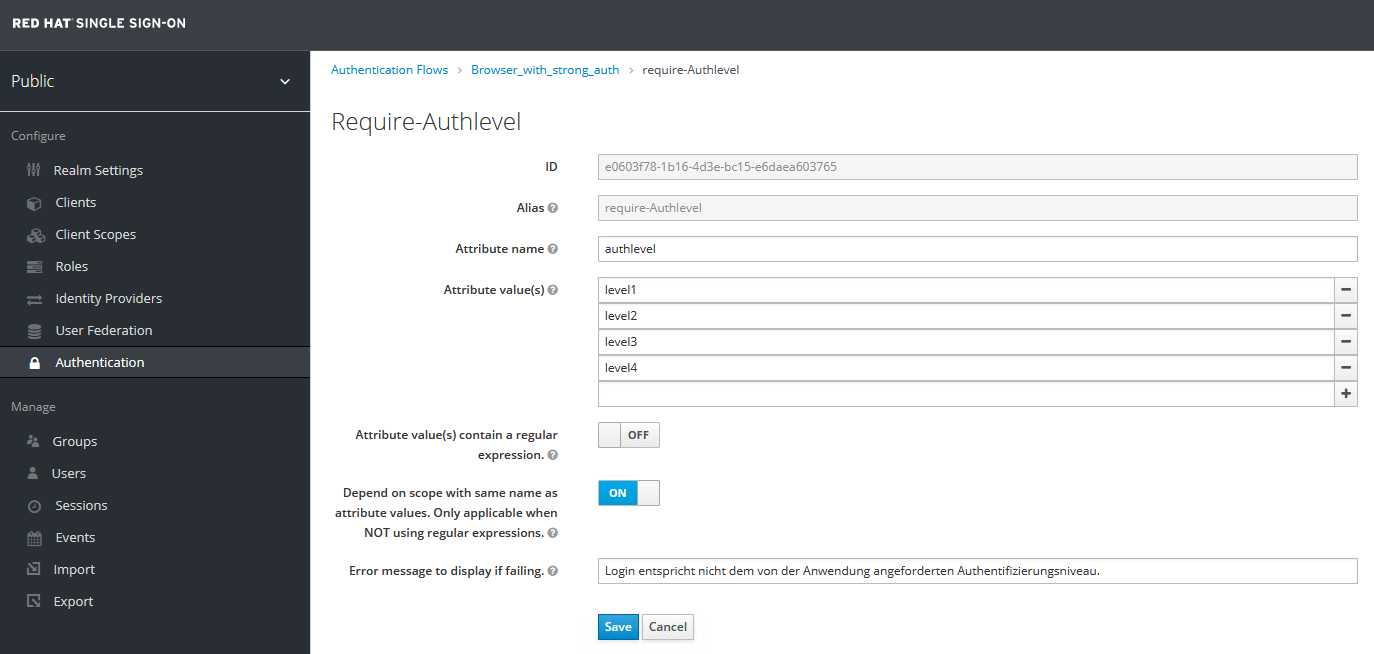


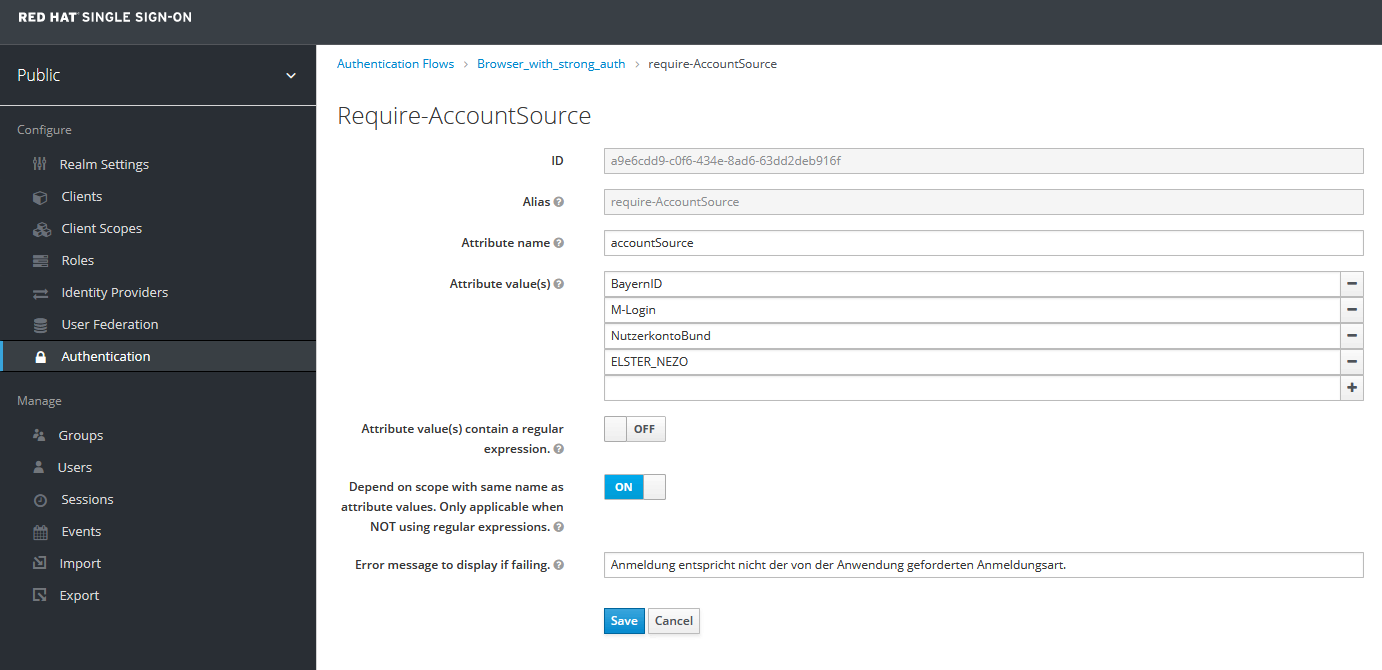
Im Beispiel sieht man hier ebenfalls „echte“ Client Scopes (authlevel\_legacy, email, profile) und Dummy Client Scopes (BayernID, level1, level2, level3, level4). Der Unterschied ist, dass man bei OIDC noch zwischen default (Attribute werden immer geliefert) und optional (Attribute werden nur bei expliziter Anforderung geliefert) Client Scopes unterschieden, wobei es bei den Dummy Client Scopes genügt, diese als optional Client Scopes zu definieren.

## Authentication Flow

Es sollte der folgende Authentication Flow angelegt werden (kann als Kopie des Standard Browser-Flow erreicht werden):







Diesen Flow als Standard-Browser-Flow setzen (oder in den gewünschten Clients setzen):

