

Konfiguration BayernID-Plugin

SAML Konfig

Identity Providers → Add provider ... → SAML v2.0

[Identity providers](#) > Provider details

Login mit BayernID

Settings

Mappers

General settings

| | |
|-----------------|---|
| Redirect URI ⓘ | <input type="text" value="https://sam1test.muenchen.de/auth/realms/demo/broker/buergerkonto/endpoint"/> |
| Alias * ⓘ | <input type="text" value="buergerkonto"/> |
| Display name ⓘ | <input type="text" value="Login mit BayernID"/> |
| Display order ⓘ | <input type="text"/> |
| Endpoints ⓘ | SAML 2.0 Service Provider Metadata |

SAML settings

| | |
|--------------------------------|--|
| Service provider entity ID ⓘ | <input type="text" value="https://sam1test.muenchen.de/auth/realms/demo"/> |
| Identity provider entity ID ⓘ | <input type="text"/> |
| Single Sign-On service URL * ⓘ | <input type="text" value="https://infra-pre-id.bayernportal.de/idp/profile/SAML2/POST/SSO"/> |
| Single logout service URL ⓘ | <input type="text"/> |
| Backchannel logout ⓘ | <input type="checkbox"/> Off |

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

Send 'id_token_hint' in
logout requests ⓘ

☒ On

Send 'client_id' in
logout requests ⓘ

☐ Off

NameID policy format
ⓘ

Unspecified ▼

Principal type ⓘ

Attribute [Friendly Name] ▼

Principal attribute ⓘ

bPK2

Allow create ⓘ

☒ On

HTTP-POST binding
response ⓘ

☒ On

HTTP-POST binding
for AuthnRequest ⓘ

☒ On

HTTP-POST binding
logout ⓘ

☐ Off

Want AuthnRequests
signed ⓘ

☒ On

Signature algorithm
ⓘ

RSA_SHA256 ▼

SAML signature key
name ⓘ

KEY_ID ▼

Want Assertions
signed ⓘ

☒ On

Want Assertions
encrypted ⓘ

☒ On

Encryption Algorithm

RSA-OAEP ▼

Force authentication ☒ On ⓘ

Validate Signatures ⓘ ☒ On

Metadata descriptor URL ⓘ

Use metadata descriptor URL ⓘ ☐ Off

Validating X509 certificates ⓘ

Sign service provider metadata ⓘ ☐ Off

Pass subject ⓘ ☐ Off

Allowed clock skew ⓘ

Attribute Consuming Service Index ⓘ

Attribute Consuming Service Name ⓘ

Requested AuthnContext Constraints

Comparison ⓘ

AuthnContext ClassRefs ⓘ [+ Add AuthnContext ClassRef](#)

AuthnContext DeclRefs ⓘ [+ Add AuthnContext DeclRef](#)

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}`

[Identity Providers](#) > [buergerkonto](#) > [Identity Provider Mappers](#) > Username

Username

ID

Name * ⓘ

Sync Mode Override * ⓘ

Mapper Type ⓘ

Template ⓘ

Target ⓘ

ID:
Name: ID
Template: \${ATTRIBUTE.bPK}

[Identity Providers](#) > [burgerkonto](#) > [Identity Provider Mappers](#) > ID

ID

| | |
|------------------------|---|
| ID | <input type="text" value="4e696b51-ef9d-4b89-8b90-4d5b3c8c6578"/> |
| Name * ? | <input type="text" value="ID"/> |
| Sync Mode Override * ? | <input type="text" value="inherit"/> |
| Mapper Type ? | <input type="text" value="Custom ID Template Importer"/> |
| Template ? | <input type="text" value="\${ATTRIBUTE.bPK}"/> |
| | <input type="button" value="Save"/> <input type="button" value="Cancel"/> |










Surname:
Name: surname
Attribute Name: urn:oid:2.5.4.4
Friendly Name: surname
User Attribute Name: lastName

Surname

| | |
|-----------------------------|---|
| ID | <input type="text" value="5f44f733-f4f3-4d75-b721-e8601027a757"/> |
| Name * ? | <input type="text" value="surname"/> |
| Sync Mode Override * ? | <input type="text" value="inherit"/> |
| Mapper Type ? | <input type="text" value="CUSTOM Attribute-with-Scope Importer"/> |
| Attribute Name ? | <input type="text" value="urn:oid:2.5.4.4"/> |
| Friendly Name ? | <input type="text" value="surname"/> |
| Name Format ? | <input type="text" value="Select One..."/> |
| User Attribute Name ? | <input type="text" value="lastName"/> |
| CUSTOM Scope ? | <input type="text" value="profile"/> |
| CUSTOM Required Attribute ? | <input type="button" value="OFF"/> |










Mail:
Name: mail
Attribute Name: urn:oid:0.9.2342.19200300.100.1.3
Friendly Name: mail
User Attribute Name: email

Mail

| | |
|---|---|
| ID | <input type="text" value="37c58057-a9a9-44b8-86a5-3bc933958257"/> |
| Name *  | <input type="text" value="mail"/> |
| Sync Mode Override *  | <input type="text" value="inherit"/> |
| Mapper Type  | <input type="text" value="CUSTOM Attribute-with-Scope Importer"/> |
| Attribute Name  | <input type="text" value="urn:oid:0.9.2342.19200300.100.1.3"/> |
| Friendly Name  | <input type="text" value="mail"/> |
| Name Format  | <input type="text" value="Select One..."/> |
| User Attribute Name  | <input type="text" value="email"/> |
| CUSTOM Scope  | <input type="text" value="email"/> |
| CUSTOM Required Attribute  | <input type="checkbox"/> OFF |
| | <input type="button" value="Save"/> <input type="button" value="Cancel"/> |

GivenName:
Name: givenName
Attribute Name: urn:oid:2.5.4.42
Friendly Name: givenName
User Attribute Name: firstName

GivenName

| | |
|---|---|
| ID | <input type="text" value="8e449702-9ee0-4265-93c8-865117d43cf3"/> |
| Name *  | <input type="text" value="givenName"/> |
| Sync Mode Override *  | <input type="text" value="inherit"/> |
| Mapper Type  | <input type="text" value="CUSTOM Attribute-with-Scope Importer"/> |
| Attribute Name  | <input type="text" value="urn:oid:2.5.4.42"/> |
| Friendly Name  | <input type="text" value="givenName"/> |
| Name Format  | <input type="text" value="Select One..."/> |
| User Attribute Name  | <input type="text" value="firstName"/> |
| CUSTOM Scope  | <input type="text" value="profile"/> |
| CUSTOM Required Attribute  | <input type="checkbox"/> OFF |
| | <input type="button" value="Save"/> <input type="button" value="Cancel"/> |

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:

| Search... | | | | Create | Add Builtin |
|-----------------------|---------------------------|----------------------------|----------------|---------|-------------|
| Name | Category | Type | Priority Order | Actions | |
| postOfficeBox | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| personalTitle | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| displayName | AttributeStatement Mapper | CUSTOM DisplayName (SAML2) | 0 | Edit | Delete |
| bPK2 | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| username | AttributeStatement Mapper | User Property | 0 | Edit | Delete |
| AssertionProvedBy | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| bPK | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| gender | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| artisticName | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| EIDAS-Issuing-Country | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| firstName | AttributeStatement Mapper | User Property | 0 | Edit | Delete |
| accountSource | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| ukHandle | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| Version | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| legacyPostkorbHandle | AttributeStatement Mapper | User Attribute | 0 | Edit | Delete |
| lastName | AttributeStatement Mapper | User Property | 0 | Edit | Delete |

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.

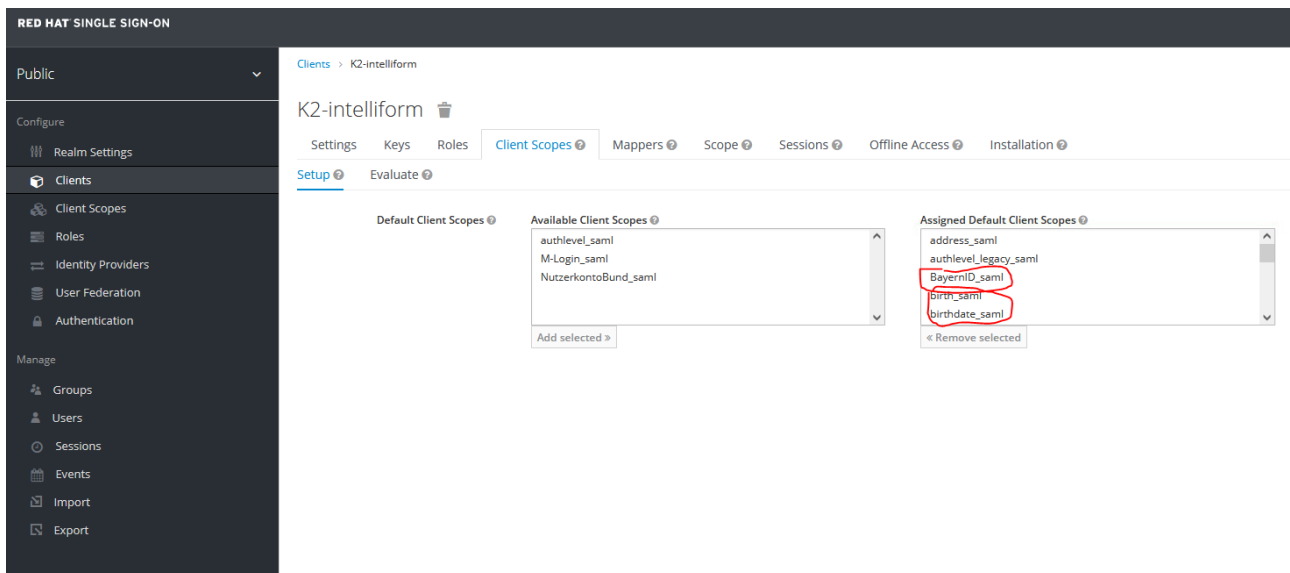
Außerdem sollte man folgende „Dummy-Scopes“ anlegen (jeweils für OIDC und für SAML2 mit Erweiterung „_saml“):

- 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

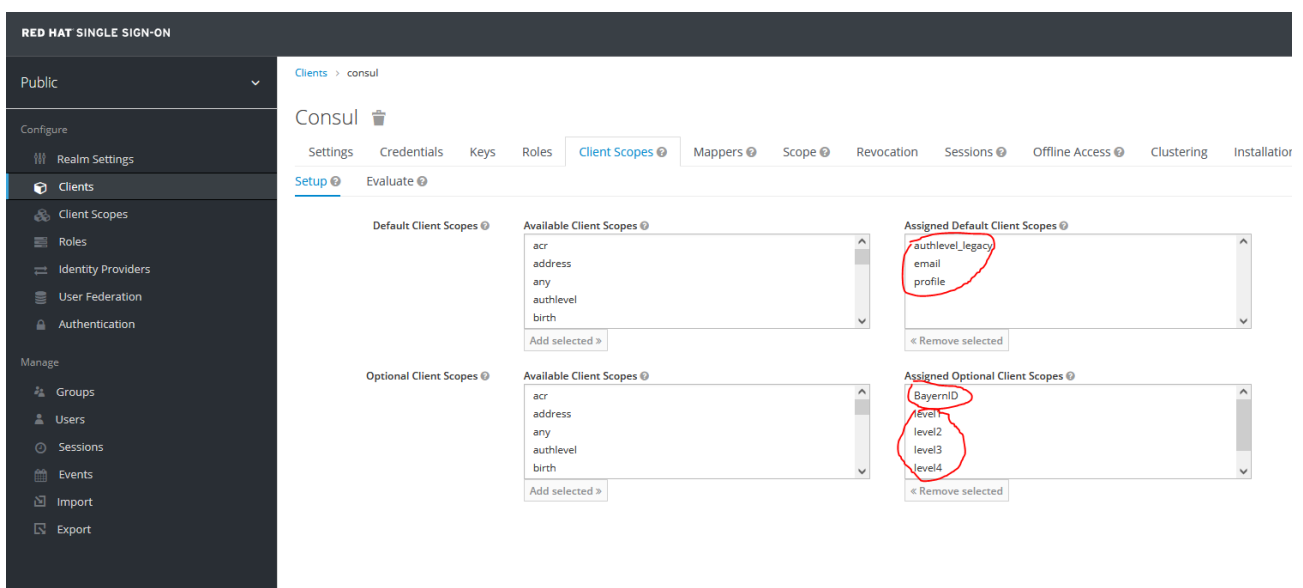
Im jeweiligen Client muss man die gewünschten Client Scopes dann explizit hinzufügen:



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):

| Auth Type | Requirement | Actions |
|--|-------------|---------|
| Browser_with_strong_auth | REQUIRED | Actions |
| Cookie-Flow | ALTERNATIVE | Actions |
| Cookie | REQUIRED | Actions |
| Require Attribute (require-Authlevel) | REQUIRED | Actions |
| Require Attribute (require-AccountSource) | REQUIRED | Actions |
| Kerberos | REQUIRED | Actions |
| CUSTOM Identity Provider Redirector | REQUIRED | Actions |
| Browser_with_strong_auth Forms | REQUIRED | Actions |
| Username Password Form | REQUIRED | Actions |
| Browser_with_strong_auth Forms - Auth-otp-form - Conditional | REQUIRED | Actions |
| Condition - User Configured | REQUIRED | Actions |
| OTP Form | REQUIRED | Actions |

Authentication Flows > Browser_with_strong_auth > require-Authlevel

Require-Authlevel

ID: e0603f78-1b16-4d3e-bc15-e6daea603765

Alias: require-Authlevel

Attribute name: authlevel

Attribute value(s): level1, level2, level3, level4

Attribute value(s) contain a regular expression: OFF

Depend on scope with same name as attribute values. Only applicable when NOT using regular expressions: ON

Error message to display if failing: Login entspricht nicht dem von der Anwendung angeforderten Authentifizierungsniveau.

Save Cancel

RED HAT SINGLE SIGN-ON

Public

Authentication Flows > Browser_with_strong_auth > require-AccountSource

Require-AccountSource

ID: a9e6cdd9-c0f6-434e-8ad6-63dd2deb916f

Alias: require-AccountSource

Attribute name: accountSource

Attribute value(s):

| | |
|-----------------|---|
| BayernID | - |
| M-Login | - |
| NutzerkontoBund | - |
| ELSTER_NEZO | - |
| | + |

Attribute value(s) contain a regular expression: OFF

Depend on scope with same name as attribute values. Only applicable when NOT using regular expressions: ON

Error message to display if failing: Anmeldung entspricht nicht der von der Anwendung geforderten Anmeldungsart.

Save Cancel

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

RED HAT SINGLE SIGN-ON

Public

Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy CIBA Policy

Browser Flow: Browser_with_strong_auth

Registration Flow: registration

Direct Grant Flow: direct grant

Reset Credentials: reset credentials

Client Authentication: clients

Save Cancel