

AW-SCIMv2-Extended - ENTWURF

IAM - Identity and Access Management

Exported on 10/10/2024

Table of Contents

1	Einleitung	5
2	Endpunkte	6
3	Benutzerattribute	8
4	OU-Permissions.....	9
5	Fehlermeldungen.....	10
6	Benutzerabfragen für Abgleich	17
6.1	Neue Benutzer.....	17
6.2	Geänderte Benutzer	17
6.3	Neue und geänderte Benutzer	17
6.4	Alle Benutzer, erste Anfrage	17
6.5	Alle Benutzer, zweite Anfrage (Pagination)	17
7	Authentifizierung	18

Status	BEARBEITUNG (see page 3)
Zielgruppe	P20 Teilnehmer
Dokumenteneigner	DI-PG-IAM
Gültig ab	
Version	0.1


Zusammenfassung	Das vorliegende Dokument beinhaltet Spezifikation der AW-SCIMv2-Extended Schnittstelle.
Einstufung der Geheimhaltung	KEINE

Inhaltsverzeichnis

- [Einleitung](#)(see page 5)
- [Endpunkte](#)(see page 6)
- [Benutzerattribute](#)(see page 8)
- [OU-Permissions](#)(see page 9)
- [Fehlermeldungen](#)(see page 10)
- [Benutzerabfragen für Abgleich](#)(see page 17)
 - [Neue Benutzer](#)(see page 17)
 - [Geänderte Benutzer](#)(see page 17)
 - [Neue und geänderte Benutzer](#)(see page 17)
 - [Alle Benutzer, erste Anfrage](#)(see page 17)
 - [Alle Benutzer, zweite Anfrage \(Pagination\)](#)(see page 17)
- [Authentifizierung](#)(see page 18)

Änderungsverzeichnis

Änderungsverzeichnis

Datum	Version	Beschreibung	Autor
 30 Sep 2024	0.1	Initiale Dokumentenerstellung	Dr. Patrik Stellmann (HH Extern) ¹

¹ <https://confluence.bka.extrapol.de/display/~hhpp106349>

Prüfverzeichnis

Prüfverzeichnis

Datum	Version	Beschreibung	Prüfer

1 Einleitung

Der Basisdienst IAM definiert gemäß [F-IAM-Gesamtkonzepte](#)² eine einheitliche SCIMv2-Schnittstelle für polizeiliche Fachanwendungen, die möglichst von sämtlichen Anwendungen mit einer IDM-Anbindung an das F-IAM genutzt werden soll. Dabei ist die Schnittstelle als Obermenge aller üblichen Anforderungen zu verstehen, von denen jede Anwendung nur den Teil umsetzt, den sie konkret benötigt.

² <https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=129107669#IAMP20Dokumenteübersicht-F-IAM-Gesamtkonzept>

2 Endpunkte

Die von der Anwendung zu unterstützenden Endpunkte hängen davon ab, ob sie AW-Rechte mit oder ohne Dienststellenbezug (oder auch beides) unterstützen.

Endpunkt	Operation	Beschreibung	relevant für AWs
/ResourceTypes	GET	Schemas, Users, Groups, ... liefert auch die URLs der Endpunkte	immer
/Schemas	GET	relevant?	immer
/Users	GET	Abfrage aller Benutzer Es müssen mindestens die folgenden Filter unterstützt werden: <ul style="list-style-type: none"> • erzeugt ab • geändert ab • ID ab (für Pagination) 	immer
	POST	Erstellen eines neuen Benutzers	immer
/Users/{User-ID}	GET	Abfrage eines konkreten Benutzers, ID wird von AW vergeben <i>Liefert auch die Liste aller Berechtigungszuweisungen (auch mit OU-Bezug), sofern es nicht über Query-Parameter unterbunden wird.</i>	immer
	PUT	Entfällt, Änderungen werden per PATCH vorgenommen	
	PATCH	Ändern von Benutzerattributen	
	DELETE	Löschen eines Benutzers	
/Groups	GET	Abfrage aller AW-Rechte ohne Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	für AW mit Berechtigungen ohne Dienststellenbezug

Endpunkt	Operation	Beschreibung	relevant für AWs
/Groups/{Group-ID}	GET	Abfrage eines konkreten AW-Rechts ohne Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	
	PATCH	Berechtigungszuweisung hinzufügen/entfernen <i>Pro Nachricht vom F-IAM wird immer nur eine einzelne Operation enthalten sein.</i>	
/OU-Permissions	GET	Abfrage aller AW-Rechte mit Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	für AW mit Berechtigungen mit Dienststellenbezug
/OU-Permissions/{OU-Permission-ID}	GET	Abfrage eines konkreten AW-Rechtes mit Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	
	PATCH	Berechtigungszuweisung mit Dienststellenbezug hinzufügen/entfernen <i>Pro Nachricht vom F-IAM wird immer nur eine einzelne Operation enthalten sein. (Zuweisen/Entziehen eines einzelnen Rechts für einen einzelnen Benutzer für eine konkrete Dienststelle</i>	

3 Benutzerattribute

Die Anwendung darf nur die Benutzerattribute speichern, für die es einen fachlichen Bedarf gibt. Das F-IAM kann dabei nur die Benutzerattribute liefern, die auch von den TN bereitgestellt wurden. Die mögliche Obermenge ist separat beschrieben: [Benutzerattribute im F-IAM](#)³

³ <https://confluence.bka.extrapol.de/x/46DMD>

4 OU-Permissions

TODO

5 Fehlermeldungen

Der AW-SCIMv2-Server soll in den folgenden Fehlerfällen die entsprechenden Fehlermeldungen zurückgeben:

- Benutzer anlegen:
 - Obligatorische Daten im User fehlen (familyName, givenName, idpUserId, p20DepartmentNumber)

HTTP/1.1 400 Bad Request
Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request failed due to invalid syntax.",
  "status": "400",
  "scimType": "invalidValue",
  "resourceType": "User",
  "errors": [
    {
      "status": "400",
      "detail": "The required attribute 'givenName' is missing.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": null
    },
    {
      "status": "400",
      "detail": "The required attribute 'familyName' is missing.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": null
    },
    {
      "status": "400",
      "detail": "The required attribute 'idpUserId' is missing.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": null
    },
    {
      "status": "400",
      "detail": "The required attribute 'p20DepartmentNumber' is missing.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": null
    }
  ]
}
```

- Benutzer besteht schon (idpUserId einen aktiven anderen Benutzer zugewiesen, falls eine idpUserId transferiert werden soll, dann muss erst die ID beim alten Benutzer gelöscht und dann beim neuen Benutzer angelegt werden)

HTTP/1.1 409 Conflict

Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with the
current state of the resource.",
  "status": "409",
  "scimType": "uniqueness",
  "resourceType": "User",
  "errors": [
    {
      "status": "409",
      "detail": "The attribute 'idpUserId' must be unique. The provided
value is already in use.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": "existing_idp_user_id"
    }
  ]
}
```

- Benutzer über SCIM aktualisieren:
 - Benutzer ist in IGVP nicht vorhanden (technische ID in IGVP nicht vorhanden)

HTTP/1.1 404 Not Found
Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "User",
  "errors": [
    {
      "status": "404",
      "detail": "The User with id 'unknown_user_id' does not exist.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": "unknown_user_id"
    }
  ]
}
```

- Benutzererkennung ist doppelt (neue idpUserId ist bereits einem anderen Benutzer zugewiesen, siehe oben)

HTTP/1.1 409 Conflict
Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
```

```

    "detail": "The request could not be completed due to a conflict with the
current state of the resource.",
    "status": "409",
    "scimType": "uniqueness",
    "resourceType": "User",
    "errors": [
      {
        "status": "409",
        "detail": "The attribute 'idpUserId' must be unique. The provided
value is already in use by another user.",
        "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
        "value": "existing_idp_user_id"
      }
    ]
  }
}

```

- Obligatorische Datenfelder verletzt (remove oder replace mit LEER-Wert wird auf obligatorische Daten - siehe oben - ausgeführt)

HTTP/1.1 400 Bad Request
Content-Type: application/json

```

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request failed due to invalid syntax.",
  "status": "400",
  "scimType": "invalidValue",
  "resourceType": "User",
  "errors": [
    {
      "status": "400",
      "detail": "The required attribute 'givenName' cannot be set to an
empty value.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": ""
    },
    {
      "status": "400",
      "detail": "The required attribute 'familyName' cannot be set to an
empty value.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": ""
    },
    {
      "status": "400",
      "detail": "The required attribute 'idpUserId' cannot be set to an
empty value.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": ""
    }
  ]
}

```

```

    "status": "400",
    "detail": "The required attribute 'p20DepartmentNumber' cannot be
set to an empty value.",
    "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
    "value": ""
  }
]
}

```

- Berechtigung zuweisen:
 - Berechtigung ohne Dst-Bezug nicht bekannt

```

HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "Group",
  "errors": [
    {
      "status": "404",
      "detail": "The Group with id 'unknown_group_id' does not exist.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
      "value": "unknown_group_id"
    }
  ]
}

```

- Berechtigung mit Dst-Bezug nicht bekannt

```

HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "OuPermission",
  "errors": [
    {
      "status": "404",
      "detail": "The OuPermission with id 'unknown_permission_id' does not
exist.",
      "schema":
"urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
      "value": "unknown_permission_id"
    }
  ]
}

```

```

    }
  ]
}

```

- OU nicht bekannt

```

HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested OU resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "OuPermission",
  "errors": [
    {
      "status": "404",
      "detail": "The OU with id 'unknown_ou_id' does not exist.",
      "schema":
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
      "value": "unknown_ou_id"
    }
  ]
}

```

- Berechtigung ohne Dst-Bezug ist schon zugewiesen

```

HTTP/1.1 409 Conflict
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with the
current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "Group",
  "errors": [
    {
      "status": "409",
      "detail": "The group with id 'group_id' is already assigned to the
user.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
      "value": "group_id"
    }
  ]
}

```

- Berechtigung mit Dst-Bezug ist schon zugewiesen

HTTP/1.1 409 Conflict

Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with the
current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "OuPermission",
  "errors": [
    {
      "status": "409",
      "detail": "The OuPermission with id 'ou_permission_id' for ou
'ou_id' is already assigned to the user.",
      "schema":
"urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
      "value": {
        "ou": "ou_id",
        "permissionId": "ou_permission_id"
      }
    }
  ]
}
```

- Berechtigung entziehen:
 - Berechtigung nicht bekannt
→ *identisch zum Zuweisen einer unbekannten Berechtigung*
 - Berechtigung ohne Dst-Bezug ist nicht zugewiesen

HTTP/1.1 409 Conflict

Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with the
current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "Group",
  "errors": [
    {
      "status": "409",
      "detail": "The group with id 'group_id' is not assigned to the
user.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
      "value": "group_id"
    }
  ]
}
```

- Berechtigung mit Dst-Bezug ist nicht zugewiesen

```

HTTP/1.1 409 Conflict
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with the
current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "OuPermission",
  "errors": [
    {
      "status": "409",
      "detail": "The OuPermission with id 'ou_permission_id' for ou
'ou_id' is not assigned to the user.",
      "schema":
"urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
      "value": {
        "ou": "ou_id",
        "permissionId": "ou_permission_id"
      }
    }
  ]
}

```

- Benutzer über SCIM abfragen
 - Benutzer-ID nicht bekannt

```

HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested user resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "User",
  "errors": [
    {
      "status": "404",
      "detail": "The User with id 'unknown_user_id' does not exist.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": "unknown_user_id"
    }
  ]
}

```


6 Benutzerabfragen für Abgleich

Beispiele für Abfragen des F-IAM bei der AW zum Abgleich der Benutzer.

6.1 Neue Benutzer

Anfrage nach Nutzern, die seit dem 01.10.2024 00:00:00 erzeugt wurden.

```
GET /Users?filter=meta.created gt "2024-10-01T00:00:00Z"
```

6.2 Geänderte Benutzer

Anfrage nach Nutzern, die seit dem 01.10.2024 00:00:00 geändert wurden.

```
GET /Users?filter=meta.lastModified gt "2024-10-01T00:00:00Z"
```

6.3 Neue und geänderte Benutzer

Anfrage nach Nutzern, die seit dem 01.10.2024 00:00:00 erzeugt oder geändert wurden.

```
GET /Users?filter=meta.created gt "2024-10-01T00:00:00Z" or meta.lastModified gt "2024-10-01T00:00:00Z"
```

6.4 Alle Benutzer, erste Anfrage

Anfrage nach allen Benutzern für einen Komplettabgleich, wobei lediglich 100 Treffer erwartet werden.

```
GET /Users?count=100
```

6.5 Alle Benutzer, zweite Anfrage (Pagination)

Anfrage nach allen Benutzern für einen Komplettabgleich, wobei lediglich 100 Treffer erwartet werden, aber beginnend ab dem Benutzer nach der ersten Abfrage.

```
GET /Users?startIndex=101&count=100
```

7 Authentifizierung

Zur Authentifizierung wird das F-IAM ein selbst ausgestelltes JWT als Bearer-Token übergeben. Die Signatur ist also gegen das OIDC-Zertifikat des F-IAM zu prüfen (siehe [Access Manager Zugangsdaten](#)⁴).

Scope und erforderliches Recht (im groups-Claim des JWT) werden bei der Anbindung individuell abgestimmt. Aus Sicht des F-IAM handelt es sich hierbei um eine andere Anwendung als für die Authentifizierung von Benutzern, die die Anwendung verwenden wollen, da die Berechtigung zum Zugriff auf die SCIMv2-Schnittstelle nicht durch die TN vergeben werden darf.

⁴ <https://confluence.bka.extrapol.de/x/MzS-CQ>