AW-SCIMv2-Extended - Version 1.0.1

P20 IAM - Identity and Access Management

Exported on 01/30/2025

Table of Contents

Status	**FREIGEGEBEN**
Zielgruppe	AW-Entwickler
Dokumenteneigner	DI-PG-IAM
Gültig ab	24 Jan 2025
Version	1.0.1

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

Inhaltsverzeichnis

Änderungsverzeichnis

Änderungsverzeichnis

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

15 Nov 2024	0.2	Korrektur nach Feedback von IGVP: • Filter auf Users nach startIndex, nicht ID • PATCH-Operationen enthalten immer nur eine Attributänderung • Weitere Beispiele für Benutzeränderungen (Eintrag in Liste, Custom-Attribut, Löschen) • Korrektur: `details` einheitlich für Rechte-Details verwendet • Korrektur: `id` statt `value` im Schema für OuPermission, analog zu Group • Korrektur: `displayName` statt `display` im Schema von OuPermission, analog zu Group, Beispiele waren schon korrekt (in Referenz-Listen wird bereits in den Core-Schemata einheitlich `display` verwendet, so dass die Extension-Schemata hier analog aufgebaut sind.) • Korrektur: Referenzen einheitlich als "$ref" (statt manchmal "ref") • "IGVP" als Anwendungsbezeichnung ersetzt durch "Anwendung" • **noch offen**: Fehlermeldung, wenn temporär an einem Benutzer keine Änderungen vorgenommen werden können (weil er gerade angemeldet ist) Korrektur nach Feedback von Artus: • excludeAttributes=members bei OuPermissions erfodert Schema als Prefix, da es kein Core-Attribut ist • Analog angepasst beim Abfragen von Groups mit Custom-Schema für details	Dr. Patrik Stellmann (HH Extern)
22 Nov 2024	0.3	Anpassungen nach Feedback von IGVP: • Korrektur: Referenz als "$ref" (statt "ref") beim Groups-Schema • Hinweis ergänzt, dass beim Abfragen von Groups je nach AW auch das das Core-Schema genutzt werden kann	Dr. Patrik Stellmann (HH Extern)
06 Dec 2024	0.4	Anpassungen nach Feedback von IGVP und Artus: • Erklärung zum Schema-Prefix vor `members` bei `excludeAttributes` für /Groups und /OuPermissions • Korrektur des Schema-Prefix (urn: fehlte)	Dr. Patrik Stellmann (HH Extern)

18 Dec 2024	0.5	Anpassungen nach Feedback von BKA-Dev: • Standard-Endpunkt ServiceProviderConfig wurde ergänzt • P20-User-Schema Amtsbezeichnung: "Verweis auf Katalog XXX" wurde rausgenommen, bis es einen TN-übergreifenden Katalog gibt, der hier referenziert werden kann. Bis dahin mus das Feld TN-individuell gefüllt werden. • Rechte-Details inkl. Custom-Group-Schema wurde entfernt, da hier weiterer Abstimmungsbedarf besteht. Das Thema ist für v1.1 vorgesehen. • Format der Fehlermeldungen wurde angepasst: Freitext ist nur in details erlaubt. Die custom-Felder errors und resourceType wurden entfernen. • Feld organizational wurde korrigiert auf organization • Pagination-Attribute in Beispielen wurden korrigiert • Korrektur der Authentifizierung: Prüfung gegen JSON-WebKey (JWK) (nicht "OIDC-Zertifikat") Anpassungen nach Feedback von IGVP und • "OuPermissions" unterhalb von User ist ein Feld und soll kleingeschrieben werden. Wurde geändert in ouPermissions. • ouPermissions ist Bestandteil der P20-Extension, wird also in den P20-User-Extension-Zweig verschoben und auch dort in das Schema aufgenommen. • Schema für OuPermissions: Verwendung von display statt displayName (wie auch bei anderen Referenzen und den Beispielen)	Dr. Patrik Stellmann (HH Extern)
19 Dec 2024	1.0	Finalisierung und Versionsfreigabe	Lars Wächtler (BKA)
24 Jan 2025	1.0.1	Korrekturen: • Verweis auf p20-Group-Schema auf Core-Groups-Schema korrigiert (unter Abfrage der AW-Rechte ohne Dst-Bezug) • "ressourceType" in einer Beispiel-Fehlermeldung entfernt • Hinweis auf Möglichkeit, weitere Fehlermeldungen in detail-Feld unterzubringen	Dr. Patrik Stellmann (HH Extern)

Prüfverzeichnis

Prüfverzeichnis

Datum	Version	Beschreibung	Prüfer
18 Dec 2024	0.5	Finale Prüfung der Schnittstellendefinition	Dieter Steding (BKA)

19 Dec 2024	1.0	Selbstprüfung	Lars Wächtler (BKA)
24 Jan 2025	1.0.1	Selbstprüfung	Dr. Patrik Stellmann (HH Extern)

1 Einleitung

Der Basisdienst IAM definiert gemäß F-IAM-Gesamtkonzepte[1] 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.

1 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, OuPermissions liefert auch die URLs der Endpunkte	immer
/Schemas	**GET**	Abfrage der Schemata	immer
/ServiceProviderConfig	**GET**	Abfrage der Features	immer
/Users	**GET**	Abfrage aller Benutzer Es müssen mindestens die folgenden Filter unterstützt werden: • erzeugt ab • geändert ab • startIndex ab (für Pagination)	immer
	POST	Erstellen eines neuen Benutzers *Beim Anlegen werden **nie** initialen Berechtigungszuweisungen angegeben. Die Pflege der Berechtigungszuweisungen erfolgt ausschließlich über die Endpunkte Groups und .*	immer
/Users/{User-ID}	**GET**	Abfrage eines konkreten Benutzers, ID wird von AW vergeben *Liefert auch die Liste aller Berechtigungszuweisungen (auch mit Dst-Bezug), sofern es nicht über Query-Parameter unterbunden wird.*	immer
	~~PUT~~	Entfällt, Änderungen werden per PATCH vorgenommen	

Endpunkt	Operation	Beschreibung	relevant für AWs
	PATCH	Ändern von Benutzerattributen *Pro Nachricht wird immer nur ein Attribut geändert.*	
	DELETE	Löschen eines Benutzers	
/Groups	**GET**	Abfrage aller AW-Rechte ohne Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	für AW mit Berechtigungen **ohne Dienststellenbezug**
/Groups/{Group-ID}	**GET**	Abfrage eines konkreten AW-Rechts ohne Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	
	PATCH	Berechtigungszuweisung hinzufügen/ entfernen *Pro Nachricht vom F-IAM wird immer nur eine einzelne Operation enthalten sein.*	
OuPermissions/	**GET**	Abfrage aller AW-Rechte mit Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	für AW mit Berechtigungen **mit** Dienststellenbezug
/OuPermissions/{OU-Permission-ID}	**GET**	Abfrage eines konkreten AW-Rechtes mit Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	

Endpunkt	Operation	Beschreibung	relevant für AWs
	PATCH	Berechtigungszuweisung mit Dienststellenbezug hinzufügen/ entfernen *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*	

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[2]

Es werden so weit wie möglich die Attribute des Standard-Schemas (`urn:ietf:params:scim:schemas:core:2.0:User`) verwendet.

Für die Attribute zum Referenzieren der hierarchischen Entität des Benutzers wird das Schema `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User` (gemäß RFC7643) verwendet, wobei nur die Attribute `organization`, `division` und `department` unterstützt werden. Diese Attribute sind veralteten sollten möglichst durch den P20-Dienststellenschlüssel ersetzt werden.

JSON-Schema "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"


```
{
  "id": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
  "name": "EnterpriseUser",
  "description": "Enterprise User",
  "attributes": [
    {
      "name": "employeeNumber",
      "type": "string",
      "multiValued": false,
      "description": "Numeric or alphanumeric identifier assigned to a person,
typically based on order of hire or association with an organization.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "costCenter",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a cost center.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
```


2 https://confluence.bka.extrapol.de/x/46DMD

```
      "name": "organization",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of an organization.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "division",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a division.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "department",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a department.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "manager",
      "type": "complex",
      "multiValued": false,
      "description": "The user's manager. A complex type that optionally allows
service providers to represent organizational hierarchy by referencing the 'id'
attribute of another User resource.",
      "required": false,
      "subAttributes": [
        {
          "name": "value",
          "type": "string",
          "multiValued": false,
          "description": "The 'id' of the SCIM resource representing the user's
manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readWrite",
          "returned": "default",
          "uniqueness": "none"
```

```
        },
        {
          "name": "$ref",
          "type": "reference",
          "referenceTypes": ["User"],
          "multiValued": false,
          "description": "The URI of the SCIM resource representing the user's
manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readWrite",
          "returned": "default",
          "uniqueness": "none"
        },
        {
          "name": "displayName",
          "type": "string",
          "multiValued": false,
          "description": "The displayName of the user's manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readOnly",
          "returned": "default",
          "uniqueness": "none"
        }
      ]
    }
  ]
}
```

Alle weiteren, P20-spezifischen Attribute sind in einem eigenen Extension-Schema `urn:ietf:params:scim:schemas:extension:p20:2.0:User` gesammelt.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:User"

```
{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
  "name": "P20User",
  "description": "Schema for P20-specific user attributes.",
  "attributes": [
    {
      "name": "idpUserName",
      "type": "string",
      "multiValued": false,
      "description": "TN-interner Nutzername",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
```

```
      "name": "idpUserId",
      "type": "string",
      "multiValued": false,
      "description": "TN-interne Nutzer-ID",
      "required": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "server"
    },
    {
      "name": "p20Uid",
      "type": "string",
      "multiValued": false,
      "description": "P20-UID",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "p20DepartmentNumber",
      "type": "string",
      "multiValued": false,
      "description": "P20-Dienststellenschlüssel, referenziert den TN-übergreifenden
Dienststellenkatalog",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "nameSuffix",
      "type": "string",
      "multiValued": false,
      "description": "P20-Namenszusatz, zur Unterscheidung von Benutzern desselben TN
mit identischem Namen",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "policeTitleKey",
      "type": "string",
      "multiValued": false,
      "description": "Schlüssel für Amtsbezeichnung",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "idp",
      "type": "string",
      "multiValued": false,
      "description": "TN-Kennung",
```

```
      "required": true,
      "mutability": "immutable",
      "returned": "default"
    },
    {
      "name": "ouPermissions",
      "type": "complex",
      "multiValued": true,
      "description": "List of assigned  for the user.",
      "required": false,
      "mutability": "readOnly",
      "subAttributes": [
        {
          "name": "id",
          "type": "string",
          "description": "Unique identifier for the OuPermission.",
          "required": true
        },
        {
          "name": "display",
          "type": "string",
          "description": "Human-readable name for the OuPermission.",
          "required": false
        },
        {
          "name": "$ref",
          "type": "reference",
          "description": "Reference to the OuPermission resource.",
          "required": false,
          "referenceTypes": ["OuPermission"]
        },
        {
          "name": "scope",
          "type": "string",
          "description": "Scope (Dienststelle) reference for the assigned
OuPermission.",
          "required": true
        },
        {
          "name": "inherit",
          "type": "boolean",
          "description": "Indicates if the permission applies to subordinate units
(Dienststellen).",
          "required": false
        }
      ]
    }
  ]
}
```

4 Berechtigungen

Bei Berechtigungen werden zwischen zwei Typen unterschieden. Dabei liegt es am Bedarf der jeweiligen Anwendung, welche davon sie verwendet (nur eine davon oder auch beide).

4.1 Groups: Berechtigungen ohne Dienststellenbezug

Berechtigungen ohne Dienststellenbezug werden durch den Resource-Typ "Group" abgebildet. Hierbei kann wahlweise der Standard-Endpunkt mit dem Standard-Schema `urn:ietf:params:scim:schemas:core:2.0:Group` verwendet werden.

4.2 OU-Permissions: Berechtigungen mit Dienststellenbezug

Berechtigungen mit Dienststellenbezug werden durch einen eigenen Resource-Type "OuPermission" abgebildet.

Mit "Dienststelle" ist hier maximal abstrakt gemeint und beschreibt eine beliebige hierarchische Entität in der Organisationsstruktur. Es kann auch ein Präsidium, eine Dienstgruppe o.ä. sein. Innerhalb des F-IAM wird nicht zwischen diesen Typen unterschieden.

Die Verwendung ist so weit wie möglich an Standard-Groups (Schema `urn:ietf:params:scim:schemas:core:2.0:Group`) angelehnt und lediglich um folgende Attribute erweitert:

- Attribute `scope` für Berechtigungszuweisungen: Enthält den P20-Dienststellenschlüssel (Referenzieren des TN-übergreifenden Dienststellenkatalogs) zur Einschränkung der Berechtigung als Freitext.
- Attribute `inherit` für Berechtigungszuweisungen: Enthält optional die Information als Boolean, ob sich die Berechtigungszuweisung auch auf untergeordnete Dienststelle beziehen soll.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"


```
{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
  "name": "OuPermission",
  "description": "Schema for managing OuPermission assignments with a scope for the
organizational unit.",
  "attributes": [
    {
      "name": "id",
      "type": "string",
      "multiValued": false,
      "description": "Unique identifier for the OuPermission.",
```

```
      "required": true,
      "mutability": "readOnly",
      "returned": "always",
      "uniqueness": "server"
    },
    {
      "name": "displayName",
      "type": "string",
      "multiValued": false,
      "description": "A human-readable name for the OuPermission.",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "members",
      "type": "complex",
      "multiValued": true,
      "description": "Users who have been assigned this OuPermission.",
      "mutability": "readWrite",
      "returned": "default",
      "subAttributes": [
        {
          "name": "value",
          "type": "string",
          "description": "The user's unique identifier.",
          "mutability": "immutable",
          "required": true
        },
        {
          "name": "display",
          "type": "string",
          "description": "A human-readable name of the member.",
          "mutability": "immutable"
        },
        {
          "name": "type",
          "type": "string",
          "description": "The type of member, always 'User'.",
          "mutability": "immutable"
        },
        {
          "name": "$ref",
          "type": "reference",
          "description": "A reference to the member resource.",
          "mutability": "immutable"
        },
        {
          "name": "scope",
          "type": "string",
          "description": "ID of the organizational unit (Dienststelle) to which this
permission applies.",
```

```
          "required": true,
          "mutability": "readWrite",
          "returned": "default"
        },
        {
          "name": "inherit",
          "type": "boolean",
          "description": "Indicates whether this permission is inherited by
subordinate organizational units (Dienststellen).",
          "mutability": "readWrite",
          "returned": "default"
        }
      ]
    }
  ]
}
```

5 Beispielnachrichten

5.1 Abfrage der AW-Rechte ohne Dst-Bezug

Anfrage

```
GET: https://.../aw/scim/Groups?excludedAttributes=members
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 2,
  "Resources": [
    {
      "id": "RECHT_1",
      "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
      ],
      "meta": {
        "resourceType": "Group",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/Groups/RECHT_1"
      },
      "displayName": "Recht eins"
    },
    {
      "id": "RECHT_2",
      "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
      ],
      "meta": {
        "resourceType": "Group",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/Groups/RECHT_2"
      },
```

```
      "displayName": "Recht zwei"
    }
  ]
}
```

5.2 Abfrage der AW-Rechte mit Dst-Bezug

Anfrage

```
GET: https://.../aw/scim/OuPermissions?
excludedAttributes=urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission:member
s
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
     "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 2,
  "Resources": [
    {
      "id": "DST_RECHT_1",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
      ],
      "meta": {
        "resourceType": "OuPermission",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/OuPermissions/DST_RECHT_1"
      },
      "displayName": "Recht mit Dst-Bezug eins"
    },
    {
      "id": "DST_RECHT_2",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
      ],
      "meta": {
        "resourceType": "OuPermission",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/OuPermissions/DST_RECHT_2"
```

```
      },
      "displayName": "Recht mit Dst-Bezug zwei"
    }
  ]
}
```

5.3 Anlegen eines Benutzers

Anfrage

```
POST: https://.../aw/scim/Users
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
Content-Length: ...
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
    "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
  ],
  "userName": "by04765432",
  "name": {
    "familyName": "Dampf",
    "givenName": "Hans"
  },
  "title": "Dr.",
  "emails": [
    {
      "primary": true,
      "type": "work",
      "value": "hans.dampf@polizei.bayern.de"
    }
  ],
  "phoneNumbers": [
    {
      "primary": true,
      "type": "work",
      "value": "+49 123 456789"
    },
    {
      "type": "fax",
      "value": "+49 987 654321"
    },
    {
      "type": "cnp",
      "value": "7-123-4567"
    }
```

```
  ],
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User":
  {
    "organization": "123",
    "division": "456",
    "department": "789"
  },
  "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
    "idpUserName": "hans.dampf@polizei.bayern.de",
    "idpUserId": "04765432",
    "p20Uid": "T-36-9-09-9876543",
    "p20DepartmentNumber": "BY-123",
    "nameSuffix": "2",
    "policeTitleKey": "123",
    "idp": "BY"
  }
}
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
    "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
  ],
  "id": "1001",
  "meta": {
    "resourceType": "User",
    "created": "2011-08-01T21:32:44.882Z",
    "lastModified": "2011-08-01T21:32:44.882Z",
    "location": "https://.../aw/scim/Users/1001"
  },
  "userName": "by04765432"
  ...
}
```

5.4 Ändern eines Benutzers

Anfrage: Nachname ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
```

```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "name.familyName",
      "value": "Dampf2"
    }
  ]
}
```

Anfrage: Telefonnummer ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "phoneNumbers[type eq \"work\"].value",
      "value": "+49 123 987654"
    }
  ]
}
```

Anfrage: P20-Dienststelle ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path":
"urn:ietf:params:scim:schemas:extension:p20:2.0:User:p20DepartmentNumber",
      "value": "BY-456"
    }
```

```
  ]
}
```

Anfrage: Abteilung löschen

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department",
      "value": ""
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

5.5 Zuweisen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "type"  : "User",
          "value" : "1001"
```

```
        }
      ]
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

5.6 Entziehen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op"   : "remove",
      "path" : "members[value eq \"1001\"]"
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

5.7 Zuweisen eines Rechts mit Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
Accept: application/scim+json
```

```
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "type": "User",
          "value": "1001",
          "scope": "09_10_0900313400000_001",
          "inherit": false
        },
        {
          "type": "User",
          "value": "1001",
          "scope": "09_10_0900987600000",
          "inherit": true
        }
      ]
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

5.8 Entziehen eines Rechts mit Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "remove",
```

```
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900313400000_001\"]"
    },
    {
      "op": "remove",
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900987600000\"]"
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

5.9 Benutzerabfragen für Abgleich

5.9.1 Neue Benutzer

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

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

5.9.2 Geänderte Benutzer

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

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

5.9.3 Neue und geänderte Benutzer

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

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

5.9.4 Alle Benutzer, erste Anfrage

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

```
GET https://.../aw/scim/Users?count=100
```

5.9.5 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 https://.../aw/scim/Users?startIndex=101&count=100
```

5.9.6 Antwort


```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 347,
  "itemsPerPage": 100,
  "startIndex": 101,
  "Resources": [
    {
      "id": "1001",
      "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User",
        "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
        "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
      ],
      "meta": {
        "resourceType": "User",
        "created": "2011-08-01T21:32:44.882Z",
        "lastModified": "2011-08-01T21:32:44.882Z",
        "location": "https://.../aw/scim/Users/1001"
      },
      "userName": "by04765432",
      "name": {
        "familyName": "Dampf",
        "givenName": "Hans"
      },
      "title": "Dr.",
      "emails": [
        {
          "primary": true,
          "type": "work",
          "value": "hans.dampf@polizei.bayern.de"
        }
      ],
```

```
"phoneNumbers": [
  {
    "primary": true,
    "type": "work",
    "value": "+49 123 456789"
  },
  {
    "type": "fax",
    "value": "+49 987 654321"
  },
  {
    "type": "cnp",
    "value": "7-123-4567"
  }
],
"groups": [
  {
    "value": "RECHT_1",
    "display": "Recht eins",
    "$ref": "https://.../aw/scim/Groups/RECHT_1",
  }
],
"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User":
{
  "organization": "123",
  "division": "456",
  "department": "789"
},
"urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
  "idpUserName": "hans.dampf@polizei.bayern.de",
  "idpUserId": "04765432",
  "p20Uid": "T-36-9-09-9876543",
  "p20DepartmentNumber": "BY-123",
  "nameSuffix": "2",
  "policeTitleKey": "123",
  "idp": "BY"
  "ouPermissions": [
    {
      "value": "DST_RECHT_1",
      "display": "Recht mit Dst-Bezug eins",
      "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
      "scope": "09_10_0900313400000_001",
      "inherit": false
    },
    {
      "value": "DST_RECHT_1",
      "display": "Recht mit Dst-Bezug eins",
      "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
      "scope": "09_10_0900987600000",
      "inherit": true
    }
  ]
```

```
        },
      },
      ...
    ]
}
```

6 Fehlermeldungen

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

Das SCIMv2-Schema für Fehlermeldungen (urn:ietf:params:scim:api:messages:2.0:Error) sieht jeweils nur einen einzelnen Fehler pro Antwort vor. Das Feld `detail` ist aber ein Freitextfeld, so dass dort auch mehrere Meldungen untergebracht werden können. Das Feld `status` kann hingegen nur einen einzelnen Wert enthalten.

Liste der Fehlermeldungen

- Benutzer anlegen:
  - Obligatorische Daten im User fehlen (familiyName, 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 required attribute 'givenName' is missing.",
  "status": "400",
  "scimType": "invalidValue"
}
```

  - 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 attribute 'idpUserId' must be unique. The provided
value is already in use.",
  "status": "409",
  "scimType": "uniqueness"
}
```

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

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

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The User with id 'unknown_user_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

- Benutzerkennung 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 attribute 'idpUserId' must be unique. The provided
value is already in use by another user.",
  "status": "409",
  "scimType": "uniqueness"
}
```

- 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 required attribute 'givenName' cannot be set to an
empty value.",
  "status": "400",
  "scimType": "invalidValue"
}
```

- 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 Group with id 'unknown_group_id' does not exist.",
```

```
  "status": "404",
  "scimType": "resourceNotFound"
}
```

- 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 OuPermission with id 'unknown_permission_id' does not
exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

- 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 OU with id 'unknown_ou_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

- 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 group with id 'group_id' is already assigned to the
user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 OuPermission with id 'ou_permission_id' for scope
'ou_id' is already assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 group with id 'group_id' is not assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

  - 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 OuPermission with id 'ou_permission_id' for scope
'ou_id' is not assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 User with id 'unknown_user_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

7 Authentifizierung

Zur Authentifizierung wird das F-IAM ein selbst ausgestelltes JWT als Bearer-Token übergeben. Die Signatur ist also gegen den JSON-WebKey (JWK) des F-IAM zu prüfen (siehe Access Manager Zugangsdaten[3]).

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 einen 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.

3 https://confluence.bka.extrapol.de/x/MzS-CQ

8 AW-SCIMv2-Extended - Version 1.0

Status	EOL (see page 38)
Zielgruppe	AW-Entwickler
Dokumenteneigner	DI-PG-IAM
Gültig ab	19 Dec 2024
Version	1.0

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

Inhaltsverzeichnis

Änderungsverzeichnis

Änderungsverzeichnis

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

15 Nov 2024	0.2	Korrektur nach Feedback von IGVP: • Filter auf Users nach startIndex, nicht ID • PATCH-Operationen enthalten immer nur eine Attributänderung • Weitere Beispiele für Benutzeränderungen (Eintrag in Liste, Custom-Attribut, Löschen) • Korrektur: `details` einheitlich für Rechte-Details verwendet • Korrektur: `id` statt `value` im Schema für OuPermission, analog zu Group • Korrektur: `displayName` statt `display` im Schema von OuPermission, analog zu Group, Beispiele waren schon korrekt (in Referenz-Listen wird bereits in den Core-Schemata einheitlich `display` verwendet, so dass die Extension-Schemata hier analog aufgebaut sind.) • Korrektur: Referenzen einheitlich als "$ref" (statt manchmal "ref") • "IGVP" als Anwendungsbezeichnung ersetzt durch "Anwendung" • **noch offen**: Fehlermeldung, wenn temporär an einem Benutzer keine Änderungen vorgenommen werden können (weil er gerade angemeldet ist) Korrektur nach Feedback von Artus: • excludeAttributes=members bei OuPermissions erfodert Schema als Prefix, da es kein Core-Attribut ist • Analog angepasst beim Abfragen von Groups mit Custom-Schema für details	Dr. Patrik Stellmann (HH Extern)
22 Nov 2024	0.3	Anpassungen nach Feedback von IGVP: • Korrektur: Referenz als "$ref" (statt "ref") beim Groups-Schema • Hinweis ergänzt, dass beim Abfragen von Groups je nach AW auch das das Core-Schema genutzt werden kann	Dr. Patrik Stellmann (HH Extern)

06 Dec 2024	0.4	Anpassungen nach Feedback von IGVP und Artus: • Erklärung zum Schema-Prefix vor `members` bei `excludeAttributes` für /Groups und /OuPermissions • Korrektur des Schema-Prefix (urn: fehlte)	Dr. Patrik Stellmann (HH Extern)

18 Dec 2024	0.5	Anpassungen nach Feedback von BKA-Dev: • Standard-Endpunkt ServiceProviderConfig wurde ergänzt • P20-User-Schema Amtsbezeichnung: "Verweis auf Katalog XXX" wurde rausgenommen, bis es einen TN-übergreifenden Katalog gibt, der hier referenziert werden kann. Bis dahin mus das Feld TN-individuell gefüllt werden. • Rechte-Details inkl. Custom-Group-Schema wurde entfernt, da hier weiterer Abstimmungsbedarf besteht. Das Thema ist für v1.1 vorgesehen. • Format der Fehlermeldungen wurde angepasst: Freitext ist nur in details erlaubt. Die custom-Felder errors und resourceType wurden entfernen. • Feld organizational wurde korrigiert auf organization • Pagination-Attribute in Beispielen wurden korrigiert • Korrektur der Authentifizierung: Prüfung gegen JSON-WebKey (JWK) (nicht "OIDC-Zertifikat") Anpassungen nach Feedback von IGVP und • "OuPermissions" unterhalb von User ist ein Feld und soll kleingeschrieben werden. Wurde geändert in ouPermissions. • ouPermissions ist Bestandteil der P20-Extension, wird also in den P20-User-Extension-Zweig verschoben und auch dort in das Schema aufgenommen. • Schema für OuPermissions: Verwendung von display statt displayName (wie auch bei anderen Referenzen und den Beispielen)	Dr. Patrik Stellmann (HH Extern)
19 Dec 2024	1.0	Finalisierung und Versionsfreigabe	Lars Wächtler (BKA)

Prüfverzeichnis

Prüfverzeichnis

Datum	Version	Beschreibung	Prüfer
18 Dec 2024	0.5	Finale Prüfung der Schnittstellendefinition	Dieter Steding (BKA)

8.1 Einleitung

Der Basisdienst IAM definiert gemäß F-IAM-Gesamtkonzepte[4] 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.

8.2 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, OuPermissions liefert auch die URLs der Endpunkte	immer
/Schemas	**GET**	Abfrage der Schemata	immer
/ServiceProviderConfig	**GET**	Abfrage der Features	immer
/Users	**GET**	Abfrage aller Benutzer Es müssen mindestens die folgenden Filter unterstützt werden: • erzeugt ab • geändert ab • startIndex ab (für Pagination)	immer

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

Endpunkt	Operation	Beschreibung	relevant für AWs
	POST	Erstellen eines neuen Benutzers *Beim Anlegen werden **nie** initialen Berechtigungszuweisungen angegeben. Die Pflege der Berechtigungszuweisungen erfolgt ausschließlich über die Endpunkte Groups und .*	immer
/Users/{User-ID}	**GET**	Abfrage eines konkreten Benutzers, ID wird von AW vergeben *Liefert auch die Liste aller Berechtigungszuweisungen (auch mit Dst-Bezug), sofern es nicht über Query-Parameter unterbunden wird.*	immer
	~~PUT~~	Entfällt, Änderungen werden per PATCH vorgenommen	
	PATCH	Ändern von Benutzerattributen *Pro Nachricht wird immer nur ein Attribut geändert.*	
	DELETE	Löschen eines Benutzers	
/Groups	**GET**	Abfrage aller AW-Rechte ohne Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	für AW mit Berechtigungen **ohne Dienststellenbezug**
/Groups/{Group-ID}	**GET**	Abfrage eines konkreten AW-Rechts ohne Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	

Endpunkt	Operation	Beschreibung	relevant für AWs
	PATCH	Berechtigungszuweisung hinzufügen/ entfernen *Pro Nachricht vom F-IAM wird immer nur eine einzelne Operation enthalten sein.*	
OuPermissions/	**GET**	Abfrage aller AW-Rechte mit Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	für AW mit Berechtigungen **mit** Dienststellenbezug
/OuPermissions/{OU-Permission-ID}	**GET**	Abfrage eines konkreten AW-Rechtes mit Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	
	PATCH	Berechtigungszuweisung mit Dienststellenbezug hinzufügen/ entfernen *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*	

8.3 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[5]

Es werden so weit wie möglich die Attribute des Standard-Schemas (`urn:ietf:params:scim:schemas:core:2.0:User`) verwendet.

Für die Attribute zum Referenzieren der hierarchischen Entität des Benutzers wird das Schema `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User` (gemäß RFC7643)

5 https://confluence.bka.extrapol.de/x/46DMD

verwendet, wobei nur die Attribute `organization`, `division` und `department` unterstützt werden. Diese Attribute sind veralteten sollten möglichst durch den P20-Dienststellenschlüssel ersetzt werden.

JSON-Schema "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"

```
{
  "id": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
  "name": "EnterpriseUser",
  "description": "Enterprise User",
  "attributes": [
    {
      "name": "employeeNumber",
      "type": "string",
      "multiValued": false,
      "description": "Numeric or alphanumeric identifier assigned to a person,
typically based on order of hire or association with an organization.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "costCenter",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a cost center.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "organization",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of an organization.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "division",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a division.",
```

```
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "department",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a department.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "manager",
      "type": "complex",
      "multiValued": false,
      "description": "The user's manager. A complex type that optionally allows
service providers to represent organizational hierarchy by referencing the 'id'
attribute of another User resource.",
      "required": false,
      "subAttributes": [
        {
          "name": "value",
          "type": "string",
          "multiValued": false,
          "description": "The 'id' of the SCIM resource representing the user's
manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readWrite",
          "returned": "default",
          "uniqueness": "none"
        },
        {
          "name": "$ref",
          "type": "reference",
          "referenceTypes": ["User"],
          "multiValued": false,
          "description": "The URI of the SCIM resource representing the user's
manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readWrite",
          "returned": "default",
          "uniqueness": "none"
        },
        {
```

```
          "name": "displayName",
          "type": "string",
          "multiValued": false,
          "description": "The displayName of the user's manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readOnly",
          "returned": "default",
          "uniqueness": "none"
        }
      ]
    }
  ]
}
```

Alle weiteren, P20-spezifischen Attribute sind in einem eigenen Extension-Schema `urn:ietf:params:scim:schemas:extension:p20:2.0:User` gesammelt.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:User"

```
{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
  "name": "P20User",
  "description": "Schema for P20-specific user attributes.",
  "attributes": [
    {
      "name": "idpUserName",
      "type": "string",
      "multiValued": false,
      "description": "TN-interner Nutzername",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "idpUserId",
      "type": "string",
      "multiValued": false,
      "description": "TN-interne Nutzer-ID",
      "required": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "server"
    },
    {
      "name": "p20Uid",
      "type": "string",
      "multiValued": false,
      "description": "P20-UID",
      "required": false,
```

```
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "p20DepartmentNumber",
      "type": "string",
      "multiValued": false,
      "description": "P20-Dienststellenschlüssel, referenziert den TN-übergreifenden
Dienststellenkatalog",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "nameSuffix",
      "type": "string",
      "multiValued": false,
      "description": "P20-Namenszusatz, zur Unterscheidung von Benutzern desselben TN
mit identischem Namen",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "policeTitleKey",
      "type": "string",
      "multiValued": false,
      "description": "Schlüssel für Amtsbezeichnung",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "idp",
      "type": "string",
      "multiValued": false,
      "description": "TN-Kennung",
      "required": true,
      "mutability": "immutable",
      "returned": "default"
    },
    {
      "name": "ouPermissions",
      "type": "complex",
      "multiValued": true,
      "description": "List of assigned  for the user.",
      "required": false,
      "mutability": "readOnly",
      "subAttributes": [
        {
          "name": "id",
          "type": "string",
```

```
          "description": "Unique identifier for the OuPermission.",
          "required": true
        },
        {
          "name": "display",
          "type": "string",
          "description": "Human-readable name for the OuPermission.",
          "required": false
        },
        {
          "name": "$ref",
          "type": "reference",
          "description": "Reference to the OuPermission resource.",
          "required": false,
          "referenceTypes": ["OuPermission"]
        },
        {
          "name": "scope",
          "type": "string",
          "description": "Scope (Dienststelle) reference for the assigned
OuPermission.",
          "required": true
        },
        {
          "name": "inherit",
          "type": "boolean",
          "description": "Indicates if the permission applies to subordinate units
(Dienststellen).",
          "required": false
        }
      ]
    }
  ]
}
```


8.4 Berechtigungen

Bei Berechtigungen werden zwischen zwei Typen unterschieden. Dabei liegt es am Bedarf der jeweiligen Anwendung, welche davon sie verwendet (nur eine davon oder auch beide).

8.4.1 Groups: Berechtigungen ohne Dienststellenbezug

Berechtigungen ohne Dienststellenbezug werden durch den Resource-Typ "Group" abgebildet. Hierbei kann wahlweise der Standard-Endpunkt mit dem Standard-Schema `urn:ietf:params:scim:schemas:core:2.0:Group` verwendet werden.

8.4.2 OU-Permissions: Berechtigungen mit Dienststellenbezug

Berechtigungen mit Dienststellenbezug werden durch einen eigenen Resource-Type "OuPermission" abgebildet.

Mit "Dienststelle" ist hier maximal abstrakt gemeint und beschreibt eine beliebige hierarchische Entität in der Organisationsstruktur. Es kann auch ein Präsidium, eine Dienstgruppe o.ä. sein. Innerhalb des F-IAM wird nicht zwischen diesen Typen unterschieden.

Die Verwendung ist so weit wie möglich an Standard-Groups (Schema `urn:ietf:params:scim:schemas:core:2.0:Group`) angelehnt und lediglich um folgende Attribute erweitert:

- Attribute `scope` für Berechtigungszuweisungen: Enthält den P20-Dienststellenschlüssel (Referenzieren des TN-übergreifenden Dienststellenkatalogs) zur Einschränkung der Berechtigung als Freitext.
- Attribute `inherit` für Berechtigungszuweisungen: Enthält optional die Information als Boolean, ob sich die Berechtigungszuweisung auch auf untergeordnete Dienststelle beziehen soll.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"


```
{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
  "name": "OuPermission",
  "description": "Schema for managing OuPermission assignments with a scope for the
organizational unit.",
  "attributes": [
    {
      "name": "id",
      "type": "string",
      "multiValued": false,
      "description": "Unique identifier for the OuPermission.",
      "required": true,
      "mutability": "readOnly",
      "returned": "always",
      "uniqueness": "server"
    },
    {
      "name": "displayName",
      "type": "string",
      "multiValued": false,
      "description": "A human-readable name for the OuPermission.",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "members",
```

```
      "type": "complex",
      "multiValued": true,
      "description": "Users who have been assigned this OuPermission.",
      "mutability": "readWrite",
      "returned": "default",
      "subAttributes": [
        {
          "name": "value",
          "type": "string",
          "description": "The user's unique identifier.",
          "mutability": "immutable",
          "required": true
        },
        {
          "name": "display",
          "type": "string",
          "description": "A human-readable name of the member.",
          "mutability": "immutable"
        },
        {
          "name": "type",
          "type": "string",
          "description": "The type of member, always 'User'.",
          "mutability": "immutable"
        },
        {
          "name": "$ref",
          "type": "reference",
          "description": "A reference to the member resource.",
          "mutability": "immutable"
        },
        {
          "name": "scope",
          "type": "string",
          "description": "ID of the organizational unit (Dienststelle) to which this
permission applies.",
          "required": true,
          "mutability": "readWrite",
          "returned": "default"
        },
        {
          "name": "inherit",
          "type": "boolean",
          "description": "Indicates whether this permission is inherited by
subordinate organizational units (Dienststellen).",
          "mutability": "readWrite",
          "returned": "default"
        }
      ]
    }
  ]
}
```

8.5 Beispielnachrichten

8.5.1 Abfrage der AW-Rechte ohne Dst-Bezug

Anfrage

```
GET: https://.../aw/scim/Groups?excludedAttributes=members
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 2,
  "Resources": [
    {
      "id": "RECHT_1",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
      ],
      "meta": {
        "resourceType": "Group",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/Groups/RECHT_1"
      },
      "displayName": "Recht eins"
    },
    {
      "id": "RECHT_2",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
      ],
      "meta": {
        "resourceType": "Group",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/Groups/RECHT_2"
      },
```

```
      "displayName": "Recht zwei"
    }
  ]
}
```

8.5.2 Abfrage der AW-Rechte mit Dst-Bezug

Anfrage

```
GET: https://.../aw/scim/OuPermissions?
excludedAttributes=urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission:members
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
     "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 2,
  "Resources": [
    {
      "id": "DST_RECHT_1",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
      ],
      "meta": {
        "resourceType": "OuPermission",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/OuPermissions/DST_RECHT_1"
      },
      "displayName": "Recht mit Dst-Bezug eins"
    },
    {
      "id": "DST_RECHT_2",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
      ],
      "meta": {
        "resourceType": "OuPermission",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/OuPermissions/DST_RECHT_2"
```

```
      },
      "displayName": "Recht mit Dst-Bezug zwei"
    }
  ]
}
```

8.5.3 Anlegen eines Benutzers

Anfrage

```
POST: https://.../aw/scim/Users
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
Content-Length: ...
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
    "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
  ],
  "userName": "by04765432",
  "name": {
    "familyName": "Dampf",
    "givenName": "Hans"
  },
  "title": "Dr.",
  "emails": [
    {
      "primary": true,
      "type": "work",
      "value": "hans.dampf@polizei.bayern.de"
    }
  ],
  "phoneNumbers": [
    {
      "primary": true,
      "type": "work",
      "value": "+49 123 456789"
    },
    {
      "type": "fax",
      "value": "+49 987 654321"
    },
    {
      "type": "cnp",
      "value": "7-123-4567"
    }
  ],
```

```
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User":
  {
    "organization": "123",
    "division": "456",
    "department": "789"
  },
  "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
    "idpUserName": "hans.dampf@polizei.bayern.de",
    "idpUserId": "04765432",
    "p20Uid": "T-36-9-09-9876543",
    "p20DepartmentNumber": "BY-123",
    "nameSuffix": "2",
    "policeTitleKey": "123",
    "idp": "BY"
  }
}
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
    "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
  ],
  "id": "1001",
  "meta": {
    "resourceType": "User",
    "created": "2011-08-01T21:32:44.882Z",
    "lastModified": "2011-08-01T21:32:44.882Z",
    "location": "https://.../aw/scim/Users/1001"
  },
  "userName": "by04765432"
  ...
}
```

8.5.4 Ändern eines Benutzers

Anfrage: Nachname ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
```

```
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "name.familyName",
      "value": "Dampf2"
    }
  ]
}
```

Anfrage: Telefonnummer ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "phoneNumbers[type eq \"work\"].value",
      "value": "+49 123 987654"
    }
  ]
}
```

Anfrage: P20-Dienststelle ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path":
"urn:ietf:params:scim:schemas:extension:p20:2.0:User:p20DepartmentNumber",
      "value": "BY-456"
    }
  ]
```

```
}
```

Anfrage: Abteilung löschen

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department",
      "value": ""
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

8.5.5 Zuweisen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "type"  : "User",
          "value" : "1001"
        }
```

```
      ]
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

8.5.6 Entziehen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op"   : "remove",
      "path" : "members[value eq \"1001\"]"
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

8.5.7 Zuweisen eines Rechts mit Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
```

```
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "type": "User",
          "value": "1001",
          "scope": "09_10_0900313400000_001",
          "inherit": false
        },
        {
          "type": "User",
          "value": "1001",
          "scope": "09_10_0900987600000",
          "inherit": true
        }
      ]
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

8.5.8 Entziehen eines Rechts mit Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "remove",
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900313400000_001\"]"
    },
```

```
    {
      "op": "remove",
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900987600000\"]"
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

8.5.9 Benutzerabfragen für Abgleich

8.5.9.1 Neue Benutzer

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

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

8.5.9.2 Geänderte Benutzer

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

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

8.5.9.3 Neue und geänderte Benutzer

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

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

8.5.9.4 Alle Benutzer, erste Anfrage

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

```
GET https://.../aw/scim/Users?count=100
```

8.5.9.5 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 https://.../aw/scim/Users?startIndex=101&count=100
```

8.5.9.6 Antwort


```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 347,
  "itemsPerPage": 100,
  "startIndex": 101,
  "Resources": [
    {
      "id": "1001",
      "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User",
        "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
        "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
      ],
      "meta": {
        "resourceType": "User",
        "created": "2011-08-01T21:32:44.882Z",
        "lastModified": "2011-08-01T21:32:44.882Z",
        "location": "https://.../aw/scim/Users/1001"
      },
      "userName": "by04765432",
      "name": {
        "familyName": "Dampf",
        "givenName": "Hans"
      },
      "title": "Dr.",
      "emails": [
        {
          "primary": true,
          "type": "work",
          "value": "hans.dampf@polizei.bayern.de"
        }
      ],
      "phoneNumbers": [
        {
          "primary": true,
```

```
        "type": "work",
        "value": "+49 123 456789"
      },
      {
        "type": "fax",
        "value": "+49 987 654321"
      },
      {
        "type": "cnp",
        "value": "7-123-4567"
      }
    ],
    "groups": [
      {
        "value": "RECHT_1",
        "display": "Recht eins",
        "$ref": "https://.../aw/scim/Groups/RECHT_1",
      }
    ],
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User":
    {
      "organization": "123",
      "division": "456",
      "department": "789"
    },
    "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
      "idpUserName": "hans.dampf@polizei.bayern.de",
      "idpUserId": "04765432",
      "p20Uid": "T-36-9-09-9876543",
      "p20DepartmentNumber": "BY-123",
      "nameSuffix": "2",
      "policeTitleKey": "123",
      "idp": "BY"
      "ouPermissions": [
        {
          "value": "DST_RECHT_1",
          "display": "Recht mit Dst-Bezug eins",
          "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
          "scope": "09_10_0900313400000_001",
          "inherit": false
        },
        {
          "value": "DST_RECHT_1",
          "display": "Recht mit Dst-Bezug eins",
          "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
          "scope": "09_10_0900987600000",
          "inherit": true
        }
      ]
    },
  },
  ...
```

```
  ]
}
```

8.6 Fehlermeldungen

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

Liste der Fehlermeldungen

- Benutzer anlegen:
  - Obligatorische Daten im User fehlen (familiyName, 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 required attribute 'givenName' is missing.",
  "status": "400",
  "scimType": "invalidValue"
}
```

  - 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 attribute 'idpUserId' must be unique. The provided
value is already in use.",
  "status": "409",
  "scimType": "uniqueness",
  "resourceType": "User"
}
```

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

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

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The User with id 'unknown_user_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound",
}
```

- Benutzerkennung 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 attribute 'idpUserId' must be unique. The provided
value is already in use by another user.",
  "status": "409",
  "scimType": "uniqueness",
}
```

- 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 required attribute 'givenName' cannot be set to an
empty value.",
  "status": "400",
  "scimType": "invalidValue"
}
```

- 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 Group with id 'unknown_group_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

  - 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 OuPermission with id 'unknown_permission_id' does not
exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

- 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 OU with id 'unknown_ou_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

- 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 group with id 'group_id' is already assigned to the
user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 OuPermission with id 'ou_permission_id' for scope
'ou_id' is already assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 group with id 'group_id' is not assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

  - 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 OuPermission with id 'ou_permission_id' for scope
'ou_id' is not assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 User with id 'unknown_user_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

8.7 Authentifizierung

Zur Authentifizierung wird das F-IAM ein selbst ausgestelltes JWT als Bearer-Token übergeben. Die Signatur ist also gegen den JSON-WebKey (JWK) des F-IAM zu prüfen (siehe Access Manager Zugangsdaten[6]).

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 einen 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.

6 https://confluence.bka.extrapol.de/x/MzS-CQ

9 AW-SCIMv2-Extended - Version 1.1 - Entwurf

Status	**BEARBEITUNG** (see page 68)
Zielgruppe	AW-Entwickler
Dokumenteneigner	DI-PG-IAM
Gültig ab	
Version	1.1-0.1

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

Inhaltsverzeichnis

Änderungsverzeichnis

Änderungsverzeichnis

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

15 Nov 2024	0.2	Korrektur nach Feedback von IGVP: • Filter auf Users nach startIndex, nicht ID • PATCH-Operationen enthalten immer nur eine Attributänderung • Weitere Beispiele für Benutzeränderungen (Eintrag in Liste, Custom-Attribut, Löschen) • Korrektur: `details` einheitlich für Rechte-Details verwendet • Korrektur: `id` statt `value` im Schema für OuPermission, analog zu Group • Korrektur: `displayName` statt `display` im Schema von OuPermission, analog zu Group, Beispiele waren schon korrekt (in Referenz-Listen wird bereits in den Core-Schemata einheitlich `display` verwendet, so dass die Extension-Schemata hier analog aufgebaut sind.) • Korrektur: Referenzen einheitlich als "$ref" (statt manchmal "ref") • "IGVP" als Anwendungsbezeichnung ersetzt durch "Anwendung" • **noch offen**: Fehlermeldung, wenn temporär an einem Benutzer keine Änderungen vorgenommen werden können (weil er gerade angemeldet ist) Korrektur nach Feedback von Artus: • excludeAttributes=members bei OuPermissions erfodert Schema als Prefix, da es kein Core-Attribut ist • Analog angepasst beim Abfragen von Groups mit Custom-Schema für details	Dr. Patrik Stellmann (HH Extern)
22 Nov 2024	0.3	Anpassungen nach Feedback von IGVP: • Korrektur: Referenz als "$ref" (statt "ref") beim Groups-Schema • Hinweis ergänzt, dass beim Abfragen von Groups je nach AW auch das das Core-Schema genutzt werden kann	Dr. Patrik Stellmann (HH Extern)

06 Dec 2024	0.4	Anpassungen nach Feedback von IGVP und Artus: • Erklärung zum Schema-Prefix vor `members` bei `excludeAttributes` für /Groups und /OuPermissions • Korrektur des Schema-Prefix (urn: fehlte)	Dr. Patrik Stellmann (HH Extern)

18 Dec 2024	0.5	Anpassungen nach Feedback von BKA-Dev: • Standard-Endpunkt ServiceProviderConfig wurde ergänzt • P20-User-Schema Amtsbezeichnung: "Verweis auf Katalog XXX" wurde rausgenommen, bis es einen TN-übergreifenden Katalog gibt, der hier referenziert werden kann. Bis dahin mus das Feld TN-individuell gefüllt werden. • Rechte-Details inkl. Custom-Group-Schema wurde entfernt, da hier weiterer Abstimmungsbedarf besteht. Das Thema ist für v1.1 vorgesehen. • Format der Fehlermeldungen wurde angepasst: Freitext ist nur in details erlaubt. Die custom-Felder errors und resourceType wurden entfernen. • Feld organizational wurde korrigiert auf organization • Pagination-Attribute in Beispielen wurden korrigiert • Korrektur der Authentifizierung: Prüfung gegen JSON-WebKey (JWK) (nicht "OIDC-Zertifikat") Anpassungen nach Feedback von IGVP und • "OuPermissions" unterhalb von User ist ein Feld und soll kleingeschrieben werden. Wurde geändert in ouPermissions. • ouPermissions ist Bestandteil der P20-Extension, wird also in den P20-User-Extension-Zweig verschoben und auch dort in das Schema aufgenommen. • Schema für OuPermissions: Verwendung von display statt displayName (wie auch bei anderen Referenzen und den Beispielen)	Dr. Patrik Stellmann (HH Extern)
19 Dec 2024	1.0	Finalisierung und Versionsfreigabe	Lars Wächtler (BKA)
19 Dec 2024	1.1-0.1	Erstellung des Dokuments zur Entwicklung der Version 1.1	Lars Wächtler (BKA)

Prüfverzeichnis

Prüfverzeichnis

Datum	Version	Beschreibung	Prüfer
18 Dec 2024	0.5	Finale Prüfung der Schnittstellendefinition	Dieter Steding (BKA)

9.1 Einleitung

Der Basisdienst IAM definiert gemäß F-IAM-Gesamtkonzepte[7] 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.

9.2 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, OuPermissions liefert auch die URLs der Endpunkte	immer
/Schemas	**GET**	Abfrage der Schemata	immer
/ServiceProviderConfig	**GET**	Abfrage der Features	immer

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

Endpunkt	Operation	Beschreibung	relevant für AWs
/Users	**GET**	Abfrage aller Benutzer Es müssen mindestens die folgenden Filter unterstützt werden: • erzeugt ab • geändert ab • startIndex ab (für Pagination)	immer
	POST	Erstellen eines neuen Benutzers *Beim Anlegen werden **nie** initialen Berechtigungszuweisungen angegeben. Die Pflege der Berechtigungszuweisungen erfolgt ausschließlich über die Endpunkte Groups und .*	immer
/Users/{User-ID}	**GET**	Abfrage eines konkreten Benutzers, ID wird von AW vergeben *Liefert auch die Liste aller Berechtigungszuweisungen (auch mit Dst-Bezug), sofern es nicht über Query-Parameter unterbunden wird.*	immer
	~~**PUT**~~	Entfällt, Änderungen werden per PATCH vorgenommen	
	PATCH	Ändern von Benutzerattributen *Pro Nachricht wird immer nur ein Attribut geändert.*	
	DELETE	Löschen eines Benutzers	
/Groups	**GET**	Abfrage aller AW-Rechte ohne Dienststellenbezug. *Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)*	für AW mit Berechtigungen **ohne Dienststellenbezug**

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

9.3 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[8]

Es werden so weit wie möglich die Attribute des Standard-Schemas (`urn:ietf:params:scim:schemas:core:2.0:User`) verwendet.

Für die Attribute zum Referenzieren der hierarchischen Entität des Benutzers wird das Schema `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User` (gemäß RFC7643) verwendet, wobei nur die Attribute `organization` , `division` und `department` unterstützt werden. Diese Attribute sind veralteten sollten möglichst durch den P20-Dienststellenschlüssel ersetzt werden.

JSON-Schema "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"


```
{
  "id": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
  "name": "EnterpriseUser",
  "description": "Enterprise User",
  "attributes": [
    {
      "name": "employeeNumber",
      "type": "string",
      "multiValued": false,
      "description": "Numeric or alphanumeric identifier assigned to a person,
typically based on order of hire or association with an organization.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "costCenter",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a cost center.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "organization",
```


8 https://confluence.bka.extrapol.de/x/46DMD

```
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of an organization.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "division",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a division.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "department",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a department.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "manager",
      "type": "complex",
      "multiValued": false,
      "description": "The user's manager. A complex type that optionally allows
service providers to represent organizational hierarchy by referencing the 'id'
attribute of another User resource.",
      "required": false,
      "subAttributes": [
        {
          "name": "value",
          "type": "string",
          "multiValued": false,
          "description": "The 'id' of the SCIM resource representing the user's
manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readWrite",
          "returned": "default",
          "uniqueness": "none"
        },
```

```
        {
          "name": "$ref",
          "type": "reference",
          "referenceTypes": ["User"],
          "multiValued": false,
          "description": "The URI of the SCIM resource representing the user's
manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readWrite",
          "returned": "default",
          "uniqueness": "none"
        },
        {
          "name": "displayName",
          "type": "string",
          "multiValued": false,
          "description": "The displayName of the user's manager.",
          "required": false,
          "caseExact": false,
          "mutability": "readOnly",
          "returned": "default",
          "uniqueness": "none"
        }
      ]
    }
  ]
}
```

Alle weiteren, P20-spezifischen Attribute sind in einem eigenen Extension-Schema `urn:ietf:params:scim:schemas:extension:p20:2.0:User` gesammelt.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:User"

```
{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
  "name": "P20User",
  "description": "Schema for P20-specific user attributes.",
  "attributes": [
    {
      "name": "idpUserName",
      "type": "string",
      "multiValued": false,
      "description": "TN-interner Nutzername",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "idpUserId",
```

```
      "type": "string",
      "multiValued": false,
      "description": "TN-interne Nutzer-ID",
      "required": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "server"
    },
    {
      "name": "p20Uid",
      "type": "string",
      "multiValued": false,
      "description": "P20-UID",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "p20DepartmentNumber",
      "type": "string",
      "multiValued": false,
      "description": "P20-Dienststellenschlüssel, referenziert den TN-übergreifenden
Dienststellenkatalog",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "nameSuffix",
      "type": "string",
      "multiValued": false,
      "description": "P20-Namenszusatz, zur Unterscheidung von Benutzern desselben TN
mit identischem Namen",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "policeTitleKey",
      "type": "string",
      "multiValued": false,
      "description": "Schlüssel für Amtsbezeichnung",
      "required": false,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "idp",
      "type": "string",
      "multiValued": false,
      "description": "TN-Kennung",
      "required": true,
```

```
      "mutability": "immutable",
      "returned": "default"
    },
    {
      "name": "ouPermissions",
      "type": "complex",
      "multiValued": true,
      "description": "List of assigned  for the user.",
      "required": false,
      "mutability": "readOnly",
      "subAttributes": [
        {
          "name": "id",
          "type": "string",
          "description": "Unique identifier for the OuPermission.",
          "required": true
        },
        {
          "name": "display",
          "type": "string",
          "description": "Human-readable name for the OuPermission.",
          "required": false
        },
        {
          "name": "$ref",
          "type": "reference",
          "description": "Reference to the OuPermission resource.",
          "required": false,
          "referenceTypes": ["OuPermission"]
        },
        {
          "name": "scope",
          "type": "string",
          "description": "Scope (Dienststelle) reference for the assigned
OuPermission.",
          "required": true
        },
        {
          "name": "inherit",
          "type": "boolean",
          "description": "Indicates if the permission applies to subordinate units
(Dienststellen).",
          "required": false
        }
      ]
    }
  ]
}
```

9.4 Berechtigungen

Bei Berechtigungen werden zwischen zwei Typen unterschieden. Dabei liegt es am Bedarf der jeweiligen Anwendung, welche davon sie verwendet (nur eine davon oder auch beide).

9.4.1 Groups: Berechtigungen ohne Dienststellenbezug

Berechtigungen ohne Dienststellenbezug werden durch den Resource-Typ "Group" abgebildet. Hierbei kann wahlweise der Standard-Endpunkt mit dem Standard-Schema `urn:ietf:params:scim:schemas:core:2.0:Group` verwendet werden.

9.4.2 OU-Permissions: Berechtigungen mit Dienststellenbezug

Berechtigungen mit Dienststellenbezug werden durch einen eigenen Resource-Type "OuPermission" abgebildet.

Mit "Dienststelle" ist hier maximal abstrakt gemeint und beschreibt eine beliebige hierarchische Entität in der Organisationsstruktur. Es kann auch ein Präsidium, eine Dienstgruppe o.ä. sein. Innerhalb des F-IAM wird nicht zwischen diesen Typen unterschieden.

Die Verwendung ist so weit wie möglich an Standard-Groups (Schema `urn:ietf:params:scim:schemas:core:2.0:Group`) angelehnt und lediglich um folgende Attribute erweitert:

- Attribute `scope` für Berechtigungszuweisungen: Enthält den P20-Dienststellenschlüssel (Referenzieren des TN-übergreifenden Dienststellenkatalogs) zur Einschränkung der Berechtigung als Freitext.
- Attribute `inherit` für Berechtigungszuweisungen: Enthält optional die Information als Boolean, ob sich die Berechtigungszuweisung auch auf untergeordnete Dienststelle beziehen soll.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"

```
{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
  "name": "OuPermission",
  "description": "Schema for managing OuPermission assignments with a scope for the
organizational unit.",
  "attributes": [
    {
      "name": "id",
      "type": "string",
      "multiValued": false,
      "description": "Unique identifier for the OuPermission.",
      "required": true,
      "mutability": "readOnly",
```

```
      "returned": "always",
      "uniqueness": "server"
    },
    {
      "name": "displayName",
      "type": "string",
      "multiValued": false,
      "description": "A human-readable name for the OuPermission.",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    },
    {
      "name": "members",
      "type": "complex",
      "multiValued": true,
      "description": "Users who have been assigned this OuPermission.",
      "mutability": "readWrite",
      "returned": "default",
      "subAttributes": [
        {
          "name": "value",
          "type": "string",
          "description": "The user's unique identifier.",
          "mutability": "immutable",
          "required": true
        },
        {
          "name": "display",
          "type": "string",
          "description": "A human-readable name of the member.",
          "mutability": "immutable"
        },
        {
          "name": "type",
          "type": "string",
          "description": "The type of member, always 'User'.",
          "mutability": "immutable"
        },
        {
          "name": "$ref",
          "type": "reference",
          "description": "A reference to the member resource.",
          "mutability": "immutable"
        },
        {
          "name": "scope",
          "type": "string",
          "description": "ID of the organizational unit (Dienststelle) to which this
permission applies.",
          "required": true,
          "mutability": "readWrite",
```

```
          "returned": "default"
        },
        {
          "name": "inherit",
          "type": "boolean",
          "description": "Indicates whether this permission is inherited by
subordinate organizational units (Dienststellen).",
          "mutability": "readWrite",
          "returned": "default"
        }
      ]
    }
  ]
}
```

9.5 Beispielnachrichten

9.5.1 Abfrage der AW-Rechte ohne Dst-Bezug

Anfrage

```
GET: https://.../aw/scim/Groups?excludedAttributes=members
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 2,
  "Resources": [
    {
      "id": "RECHT_1",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
      ],
      "meta": {
        "resourceType": "Group",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
```

```
        "location": "https://.../aw/scim/Groups/RECHT_1"
      },
      "displayName": "Recht eins"
    },
    {
      "id": "RECHT_2",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
      ],
      "meta": {
        "resourceType": "Group",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/Groups/RECHT_2"
      },
      "displayName": "Recht zwei"
    }
  ]
}
```

9.5.2 Abfrage der AW-Rechte mit Dst-Bezug

Anfrage

```
GET: https://.../aw/scim/OuPermissions?
excludedAttributes=urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission:members
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
     "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 2,
  "Resources": [
    {
      "id": "DST_RECHT_1",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
      ],
      "meta": {
        "resourceType": "OuPermission",
        "created": "2024-10-09T15:00:00Z",
```

```
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/OuPermissions/DST_RECHT_1"
      },
      "displayName": "Recht mit Dst-Bezug eins"
    },
    {
      "id": "DST_RECHT_2",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
      ],
      "meta": {
        "resourceType": "OuPermission",
        "created": "2024-10-09T15:00:00Z",
        "lastModified": "2024-10-09T15:00:00Z",
        "location": "https://.../aw/scim/OuPermissions/DST_RECHT_2"
      },
      "displayName": "Recht mit Dst-Bezug zwei"
    }
  ]
}
```

9.5.3 Anlegen eines Benutzers

Anfrage

```
POST: https://.../aw/scim/Users
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
Content-Length: ...
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
    "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
  ],
  "userName": "by04765432",
  "name": {
    "familyName": "Dampf",
    "givenName": "Hans"
  },
  "title": "Dr.",
  "emails": [
    {
      "primary": true,
      "type": "work",
      "value": "hans.dampf@polizei.bayern.de"
    }
  ],
```

```
  "phoneNumbers": [
    {
      "primary": true,
      "type": "work",
      "value": "+49 123 456789"
    },
    {
      "type": "fax",
      "value": "+49 987 654321"
    },
    {
      "type": "cnp",
      "value": "7-123-4567"
    }
  ],
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User":
  {
    "organization": "123",
    "division": "456",
    "department": "789"
  },
  "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
    "idpUserName": "hans.dampf@polizei.bayern.de",
    "idpUserId": "04765432",
    "p20Uid": "T-36-9-09-9876543",
    "p20DepartmentNumber": "BY-123",
    "nameSuffix": "2",
    "policeTitleKey": "123",
    "idp": "BY"
  }
}
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
    "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
  ],
  "id": "1001",
  "meta": {
    "resourceType": "User",
    "created": "2011-08-01T21:32:44.882Z",
    "lastModified": "2011-08-01T21:32:44.882Z",
    "location": "https://.../aw/scim/Users/1001"
  },
  "userName": "by04765432"
```

```
  ...
}
```

9.5.4 Ändern eines Benutzers

Anfrage: Nachname ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "name.familyName",
      "value": "Dampf2"
    }
  ]
}
```

Anfrage: Telefonnummer ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "phoneNumbers[type eq \"work\"].value",
      "value": "+49 123 987654"
    }
  ]
}
```

Anfrage: P20-Dienststelle ändern

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path":
"urn:ietf:params:scim:schemas:extension:p20:2.0:User:p20DepartmentNumber",
      "value": "BY-456"
    }
  ]
}
```

Anfrage: Abteilung löschen

```
PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department",
      "value": ""
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

9.5.5 Zuweisen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "type"  : "User",
          "value" : "1001"
        }
      ]
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

9.5.6 Entziehen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op"   : "remove",
      "path" : "members[value eq \"1001\"]"
    }
```

```
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

9.5.7 Zuweisen eines Rechts mit Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "type": "User",
          "value": "1001",
          "scope": "09_10_0900313400000_001",
          "inherit": false
        },
        {
          "type": "User",
          "value": "1001",
          "scope": "09_10_0900987600000",
          "inherit": true
        }
      ]
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

9.5.8 Entziehen eines Rechts mit Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8......
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "remove",
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900313400000_001\"]"
    },
    {
      "op": "remove",
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900987600000\"]"
    }
  ]
}
```

Antwort

```
HTTP/1.1 204 No Content
```

9.5.9 Benutzerabfragen für Abgleich

9.5.9.1 Neue Benutzer

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

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

9.5.9.2 Geänderte Benutzer

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

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

9.5.9.3 Neue und geänderte Benutzer

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

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

9.5.9.4 Alle Benutzer, erste Anfrage

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

```
GET https://.../aw/scim/Users?count=100
```

9.5.9.5 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 https://.../aw/scim/Users?startIndex=101&count=100
```

9.5.9.6 Antwort

```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 347,
  "itemsPerPage": 100,
  "startIndex": 101,
  "Resources": [
    {
      "id": "1001",
```

```
"schemas": [
  "urn:ietf:params:scim:schemas:core:2.0:User",
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
  "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
],
"meta": {
  "resourceType": "User",
  "created": "2011-08-01T21:32:44.882Z",
  "lastModified": "2011-08-01T21:32:44.882Z",
  "location": "https://.../aw/scim/Users/1001"
},
"userName": "by04765432",
"name": {
  "familyName": "Dampf",
  "givenName": "Hans"
},
"title": "Dr.",
"emails": [
  {
    "primary": true,
    "type": "work",
    "value": "hans.dampf@polizei.bayern.de"
  }
],
"phoneNumbers": [
  {
    "primary": true,
    "type": "work",
    "value": "+49 123 456789"
  },
  {
    "type": "fax",
    "value": "+49 987 654321"
  },
  {
    "type": "cnp",
    "value": "7-123-4567"
  }
],
"groups": [
  {
    "value": "RECHT_1",
    "display": "Recht eins",
    "$ref": "https://.../aw/scim/Groups/RECHT_1",
  }
],
"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User":
{
  "organization": "123",
  "division": "456",
  "department": "789"
},
```

```
      "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
        "idpUserName": "hans.dampf@polizei.bayern.de",
        "idpUserId": "04765432",
        "p20Uid": "T-36-9-09-9876543",
        "p20DepartmentNumber": "BY-123",
        "nameSuffix": "2",
        "policeTitleKey": "123",
        "idp": "BY"
        "ouPermissions": [
          {
            "value": "DST_RECHT_1",
            "display": "Recht mit Dst-Bezug eins",
            "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
            "scope": "09_10_0900313400000_001",
            "inherit": false
          },
          {
            "value": "DST_RECHT_1",
            "display": "Recht mit Dst-Bezug eins",
            "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
            "scope": "09_10_0900987600000",
            "inherit": true
          }
        ]
      },
    },
    ...
  ]
}
```

9.6 Fehlermeldungen

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

Liste der Fehlermeldungen

- Benutzer anlegen:
  - Obligatorische Daten im User fehlen (familiyName, 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 required attribute 'givenName' is missing.",
  "status": "400",
  "scimType": "invalidValue"
}
```

- 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 attribute 'idpUserId' must be unique. The provided
value is already in use.",
  "status": "409",
  "scimType": "uniqueness",
  "resourceType": "User"
}
```

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

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

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The User with id 'unknown_user_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound",
}
```

  - Benutzerkennung 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 attribute 'idpUserId' must be unique. The provided
value is already in use by another user.",
  "status": "409",
  "scimType": "uniqueness",
}
```

  - 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 required attribute 'givenName' cannot be set to an
empty value.",
  "status": "400",
  "scimType": "invalidValue"
}
```

- 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 Group with id 'unknown_group_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

  - 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 OuPermission with id 'unknown_permission_id' does not
exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

  - 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 OU with id 'unknown_ou_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
```

```
}
```

- 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 group with id 'group_id' is already assigned to the
user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 OuPermission with id 'ou_permission_id' for scope
'ou_id' is already assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 group with id 'group_id' is not assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

  - 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 OuPermission with id 'ou_permission_id' for scope
'ou_id' is not assigned to the user.",
  "status": "409",
  "scimType": "conflict"
}
```

- 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 User with id 'unknown_user_id' does not exist.",
  "status": "404",
  "scimType": "resourceNotFound"
}
```

9.7 Authentifizierung

Zur Authentifizierung wird das F-IAM ein selbst ausgestelltes JWT als Bearer-Token übergeben. Die Signatur ist also gegen den JSON-WebKey (JWK) des F-IAM zu prüfen (siehe Access Manager Zugangsdaten[9]).

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 einen 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.

9 https://confluence.bka.extrapol.de/x/MzS-CQ