OS2faktor Login

AuditLog API

Version: 1.0.0
Date: 26.07.2022
Author: BSG

1 Formål

Dette dokument beskriver de API snitflader der findes på OS2faktor Login til at udlæse auditlog records fra systemet.

2 Adgangskontrol

Når man kalder servicen skal man angive en API nøgle som en HTTP Header. Denne udleveres af Digital Identity når man skal have adgang til API'et. Headeren hedder ApiKey, og API nøglen angives som direkte værdi, fx

```
ApiKey: 09fc50d5-f9f6-44e1-ba63-524c146354ad
```

3 Endpoints

API'et er udstillet under det domæne hvor administratorpotalen er udstillet, fx

https://login.kommune.dk/

De enkelte API endpoints er

3.1 HTTP GET /api/auditlog/head

Dette endpoint returnerer ID'et på den nyeste auditlog-record, og formålet med endpointet er at have en hurtig måde at checke om der er kommet nye auditlogs siden man kaldte sidste gang. Denne operation er billig og hurtig at kalde, og det anbefales at man anvender den periodisk til at checke om der er nye data.

Eksempel output

```
{
  "head": 7192
}
```

Hvis man gemmer ID'erne på de auditlog records man har synkroniseret ud lokalt, så kan man nemt verificere om der er nye records i OS2faktor der skal læses ud. ID'erne er stigende, men der er ingen garanti for at de stiger med 1 for hver record (de kan hoppe med 1-3 værdipoint for hver record, afhængig af hvilken node i clusteret der danner recorden, men de er altid stigende).

3.2 HTTP GET /api/auditlog/read?offset=xxx

Dette API endpoint henter op til 100 auditlog records (hvis der er færre end 100 records, hentes kun det antal der er tilgængelige).

Som argument anvendes offset, der er ID'et på den seneste auditlog record man har udlæst. Hvis man fx har udlæst alle auditlog records til og med den med ID 7192, så kan man kalde med

GET /api/auditlog/read?offset=7192

Og så henter den de næste 100 auditlog records der har et ID større end 7192 (fortløbende). Man kan kalde endpointet fortløbende med stigende offsets for at få læst alle nye auditlog records ud.

Da der kan være mange millioner auditlog records, anbefales det at man ikke starter fra 0 og udlæser alle data hver gang, men at man holder en lokal kopi af auditlog records fx i en database.

Eksempel output


```
[ {
    "id": 18697,
    "tts": "2022-07-26T06:50:55",
    "ipAddress": "127.0.0.1",
    "correlationId": "a119db568ae33ea66932f8b8df29435b903029e6",
    "personId": 340,
    "personName": "Test Testesen",
    "cpr": "0101018081",
    "performerId": null,
    "performerName": null,
    "logAction": "LOGIN",
    "message": "Login til OS2rollekatalog",
    "personDomain": "kommune.dk",
    "samaccountName": "bsg",
    "detailType": "XML",
    "detailContent": "<?xml …",
    "detailSupplement": null
  } ]
```


Output er altid er array af auditlog records, og de enkelte felter er beskrevet nedenfor

Felt	Type	Beskrivelse
id	Integer	Er det unikke ID på denne auditlog record, og kan fx anvendes til at identificere næste offset i senere udlæsninger
tts	Timestamp (som streng)	Timestamp på hvornår hændelsen indtraf
ipAddress	Streng	IP adressen på den der udførte handlingen
correlationId	Streng	Et ID der kan bruges til at samkøre auditlog records der er udført i samme session
personId	Integer	Det unikke (interne) ID på den person som auditloggen handler om (den som handlingen er udført på/for)
personName	Streng	Navnet på den person som handlingen er udført på/for
cpr	Streng	CPR nummeret på den person som handlingen er udfort på/for
performerId	Integer	Det unikke (interne) ID på den person som har udført handlingen (fx en administrator). Dette felt kan være tomt hvis det ikke er en 3.part som har udført handlingen på vegne af den faktiske person
performerName	Streng	Navnet på den som har udført handlingen (se ovenfor)
logAction	Streng (enum)	ID på den handling der er udført – se en ikke-udtømmende liste nedenfor (listen udvides løbende når nye handlinger

		auditlogges, så det anbefales at man gemmer denne værdi som en Streng og ikke en enum i ens lokale database)
Message	Streng	Kort beskrivelse af handlingen
personDomain	Streng	Domæne ID'et på personen som handlingen udføres på/for
samaccountName	Streng	BrugerID'et på den person som handlingen udføres på/for
detailType	Streng (enum)	En angivelse af det format som detailContent og detailtSupplement er gemt i (se nedenfor)
detailContent	Streng (kan være stor)	Hvis auditlog recorden har supplerende detaljer, så angives de her. Bemærk at feltet kan være ret stort (fx auditlogges det fulde SAML token i dette felt)
detailSupplement	Streng (kan være stor)	Hvis der er supplerende data til ovenstående, så tilføjes de her

Mulige formater (detailType) er

- JSON
- XML
- TEXT