

# Attribútum\_kiadás

!!! bug "Elavult információ"

**\*\*Figyelem\*\*:** a Shibboleth szoftver ezen változata már nem támogatott. Az új verziókhoz a leírások itt találhatóak:

\* [Shibboleth2\_IdP](https://help.edu.hu/books/aai/page/shibboleth2-idp)

\* [Shibboleth2\_SP](https://help.edu.hu/books/aai/page/shibboleth2-sp)

Az Attribute Release Policy (ARP) határozza meg, hogy az attribútum feloldás után rendelkezésre álló attribútumok közül mely attribútumokat lehet az SP-nek kiadni. Egy ARP vonatkozhat a teljes IdP-re ("site" ARP), illetve az azonosított felhasználóra is. A site-ARP-k általában a **arps/arp.site.xml** állományban, a felhasználói ARP-k pedig az **arps/arp.user.\$PRINCIPAL.xml** állományban találhatóak, ahol \$PRINCIPAL megegyezik a REMOTE\_USER változóban megkapott értékkel.

## Működő példa

```
<?xml version="1.0" encoding="UTF-8"?>
<AttributeReleasePolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns="urn:mace:shibboleth:arp:1.0"
  xsi:schemaLocation="urn:mace:shibboleth:arp:1.0 shibboleth-arp-1.0.xsd" >
  <Description>Not The Simplest Possible ARP.</Description>
  <Rule>
    <Description>Mindenkire vonatkozó szabályok</Description>
    <Target>
      <AnyTarget/>
    </Target>
    <Attribute name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation">
      <AnyValue release="permit"/>
    </Attribute>
    <Attribute name="urn:mace:dir:attribute-def:eduPersonOrgDN">
      <AnyValue release="permit"/>
    </Attribute>
```

```

</Rule>
<Rule>
  <Description>NIFI által üzemeltetett SP-kre vonatkozó szabályok</Description>
  <Target>
    <Requester matchFunction="urn:mace:shibboleth:arp:matchFunction:regexMatch">.*\.n?iif\.hu\/.*</Requester>
  </Target>
  <Attribute name="urn:mace:dir:attribute-def:eduPersonPrincipalName">
    <AnyValue release="permit"/>
  </Attribute>
  <Attribute name="urn:mace:dir:attribute-def:mail">
    <AnyValue release="permit"/>
  </Attribute>
  <Attribute name="urn:mace:dir:attribute-def:cn">
    <AnyValue release="permit"/>
  </Attribute>
  <Attribute name="urn:mace:dir:attribute-def:eduPersonEntitlement">
    <Value release="permit"
      matchFunction="urn:mace:shibboleth:arp:matchFunction:regexMatch">
      ^urn:niif.hu:services:aai:entitlement:.*
    </Value>
  </Attribute>
</Rule>
</AttributeReleasePolicy>

```

# ARP feldolgozás menete

Az Attribute Authority a rendelkezésre álló ARP-kból (tehát site és felhasználói ARP-kból) egy ún. **effective ARP**-t állít elő.

1. Meghatározza, hogy melyik ARP file-okat kell feldolgozni.
2. Meghatározza, hogy melyek azok a szabályok, amelyek az attribútum lekérdezéshez kapcsolódnak
  - Minden ARP szabály, amely alapértelmezettnek vannak megjelölve, automatikusan bekerül az ARP-be, anélkül, hogy az illesztési függvényeket (matchFunction) végrehajtaná
  - Minden nem alapértelmezett szabály illesztési függvénye alapján megállapítja, hogy a providerId alapján vonatkozik-e a kérést indító félre.
3. Attribútum filter létrehozása
  1. Minden attribútumhoz megállapítja a vonatkozó Rule-ok listáját

2. Ebből a listából az összes olyan attribútum értéket kiveszi, amelyre *deny* szabály vonatkozik
3. Ha egy szabály úgy rendelkezik, hogy minden érték kiadható, akkor az egyes értékekre vonatkozó *deny* szabályok szűkítik a kiadható értékek listáját. Ha egy szabály az attribútumok összes értékének kiadását megtiltja, akkor az egyes értékekre vonatkozó engedélyek figyelmen kívül lesznek hagyva.

# ARP Rule

Az ARP szabályok különböző illeszkedési vizsgálatok segítségével megállapítják, hogy egy SP-nek egy-egy attribútum milyen feltételekkel adható ki.

## matchFunction

Ez az attribútum adja meg, hogy milyen illesztési eljárást kell használni az illeszkedési vizsgálatnál. Lehetséges értékei:

- **urn:mace:shibboleth:arp:matchFunction:stringMatch:** *true*, ha két karakterlánc pontosan megegyezik (ez az alapértelmezett illesztési függvény)
  - ugyanezt jelenti: **urn:mace:shibboleth:arp:matchFunction:exactShar**
- **urn:mace:shibboleth:arp:matchFunction:stringNotMatch:** *true*, ha két karakterlánc eltér
- **urn:mace:shibboleth:arp:matchFunction:regexMatch:** *true*, ha a karakterlánc megfelel a paraméterként megadott reguláris kifejezésnek
- **urn:mace:shibboleth:arp:matchFunction:regexNotMatch:** *true*, ha a karakterlánc nem felel meg a paraméterként megadott reguláris kifejezésnek
- **urn:mace:shibboleth:arp:matchFunction:anyValueMatch:** tetszőleges nem üres string esetén *true*

## Target

A Target elemnek kétféle gyermeke lehet:

- **\*\*AnyTarget\*\***: minden SP-re vonatkozik a szabály (az azonosíthatatlan SP-kre is!)
- **\*\*Requester\*\***: a szabály akkor kerül az effective ARP-be, ha az SP providerId-je illeszkedik

## Attribute

Egy Rule 0 vagy több Attribute elemet tartalmazhat. Tartalmaznia kell egy `name` paramétert, amely az attribútum teljes neve (általában URN, lásd az [attribútum feloldás leírását](#)). Az elemnek kétféle gyermeke lehet:

- `**AnyValue**`: az attribútum bármely értékére vonatkozik a szabály
- `**Value**`: ebben az esetben kötelezően szerepel egy `**release**` paraméter, melynek értéke *permit* vagy *deny* lehet. Itt is opcionálisan megadható a `**matchFunction**` paraméter.

## Constraint

A Constraint-ek használatával attribútumok kiadását más attribútumok értékéhez is köthetjük, így pl. megtehetjük, hogy a "hozzajarulasBeszerezve" nevű attribútum `true` értékéhez kössük az attribútumok kiadását.

A megkötések konfigurációjához lásd: <https://spaces.internet2.edu/display/SHIB/ArpConstraint>

## Tesztelés

A Shibboleth IdP-hez tartozik egy **resolvertest** névre hallgató program, amellyel ellenőrizhetjük az attribútumok kiadását is. Használatához először be kell állítani a telepítésnek megfelelően az IDP\_HOME és a JAVA\_HOME változókat.

Példa: `/usr/local/shibboleth-idp/bin/resolvertest --idpXml=file:///etc/shibboleth-idp/idp.xml --user=bajnokk`  
(Azonosítatlan SP-nek kiadott attribútumok)

```
<Attribute xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  AttributeName="urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
  AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
  <AttributeValue Scope="niif.hu">employee</AttributeValue>
</Attribute>

<Attribute xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  AttributeName="urn:mace:dir:attribute-def:eduPersonOrgDN"
  AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
  <AttributeValue>o=niifi,o=niif,c=hu</AttributeValue>
</Attribute>
```

Példa 2.: `/usr/local/shibboleth-idp/bin/resolvertest --idpXml=:///etc/shibboleth-idp/idp.xml --user=bajnokk --requester=https://dev.aai.niif.hu/shibboleth` (Azonosított SP-nek kiadott attribútumok.)

```
...
<Attribute xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
  AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
  <AttributeValue Scope="niif.hu">bajnokk</AttributeValue>
</Attribute>
...
```

# Hivatkozások

- <https://spaces.internet2.edu/display/SHIB/IdPARPConfig>
- <https://spaces.internet2.edu/display/SHIB/AttributeReleaseRule>
- <https://spaces.internet2.edu/display/SHIB/ArpConstraint>
- [ShARPE ARP Editor](#)

---

Változat #3

cziernorbert hozta létre 9 április 2025 16:36:26

cziernorbert frissítette 10 április 2025 09:54:29