



SWAMID

Swedish Academic Identity Federation

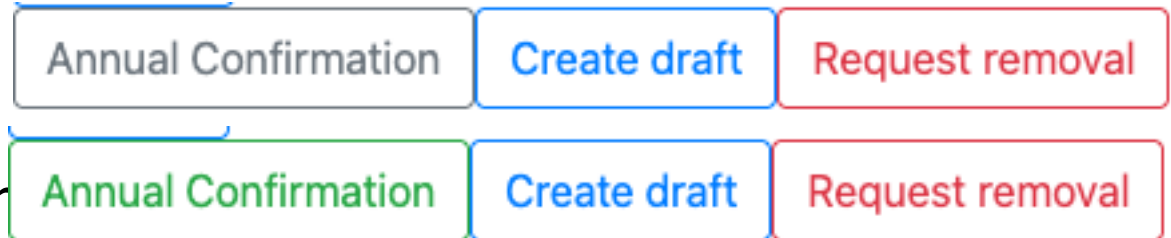
Vad har hänt / ändrats?

**Gällande metadata, release-check,
MFA i Shibboleth samt ADFS Toolkit**

Sunetdagarna våren 2025

Metadata - påminnelser

- Årskontrollen metadata
 - Mail till admin(s) av entiteten efter 10 och 11 månader (sedan sept 2024)
 - Mail + teknisk och administrativ kontakt efter 12 månader
 - Plockas bort efter ~ 13 månader
- Certifikat
 - 1 månad innan certet går ut (adr
 - När certet har gått ut (+ teknisk och administrativ kontakt)
 - Entiteten raderas ~ 1 månad efter certets utgång om inget nytt är på plats.
- Gamla Pending och Draft



Metadata – påminnelser (2)

- IMPS
 - Ny check sedan Jan 2025
 - Går till IdP-admin

IMPS

Blekinge tekniska högskola

- Accepted by Board of Trustees : 2020-12-14
- Last validated : 2020-12-14
- Last validated by : (BoT)

Updated IMPS required!

Current approved IMPS is based on a earlier version of the assurance profile.

EntityAttributes

IMPS

EntityAttributes

IMPS

Vetenskapsrådet - SUNET

- Accepted by Board of Trustees : 2023-06-21
- Last validated : 2023-06-21
- Last validated by : (BoT)

Validate

EntityAttributes

IMPS

Vetenskapsrådet - SUNET

- Accepted by Board of Trustees : 2023-06-21
- Last validated : 2024-10-02
- Last validated by : Björn Mattsson (bjorn@sunet.se)

Validate

EntityAttributes

Metadata - SeamlessAccess

- SeamlessAccess integrering

- Profiler / IdP filtering

(<https://wiki.sunet.se/display/SWAMID/3.6+Identity+Provider+Discovery>)

- <https://service.seamlessaccess.org/ds/?trustProfile=edugain>
 - Måste läggas till i metadata för SP !!!!
 - Går att redigera i metadata.swamid

- SA klagar om DiscoveryResponse saknas / är fel

(<https://wiki.sunet.se/display/SWAMID/DiscoveryResponse>)

- Under en period klagade metadata.swamid om den saknades. Detta är nu avstängt
 - Går numera att redigera

entity-category

- <http://refeds.org/category/research-and-scholarship>
- <https://refeds.org/category/code-of-conduct/v2>
- <https://refeds.org/category/personalized>

entity-selection-profile

- edugain

- entity-selection-profile

- [\[set\]](#) swamid - Registered in SWAMID
 - [\[set\]](#) edugain - Registered in SWAMID or imported from eduGAIN

DiscoveryResponse

- **Index = 1**
<https://release-check.swamid.se/Shibboleth.sso/Login>
- **Index = 2**
<https://release-check.swamid.se/Shibboleth.sso/DS/swamid-test>
- **Index = 3**
<https://release-check.swamid.se/Shibboleth.sso/DS/seamless-access>

Metadata - Övrigt

- Samarbete med andra Federationer
 - Nya Zeeland
 - Deltar aktivt i utvecklingen
 - Kanada
 - Visat intresse men inte haft tid att gå in
- Kontroll av e-mailadresser
 - Kommer "snart" att börja testa att samtliga adresser i Metadata är nåbara
 - Verifiering var 12 månad
 - Förslag på något bättre än ett mail med en länk ?

Release-check

4 flikar :

- Attributes
 - Logga in och visa vilka attribute som IdP:n skickar
- MFA
 - Testar support för REFEDS MFA och ForceAuthn.
- ESI
 - Testar support för European Student Identifier

Release-check – vad gör den ?

- Entity category
 - Dessa tester skall köras en gång per år
 - Synkroniseras över till metadata.swamid
 - Tester
 - assurance - eduPersonAssurance och värden
 - noec - inga värden skall skickas !
 - anonymous - REFEDS Anonymous Access
 - pseudonymous - REFEDS Pseudonymous Access
 - personalized - REFEDS Personalized Access
 - cocov2-1, cocov2-2 - REFEDS CoCo (v2)
 - cocov2-3 - REFEDS CoCo (v2) utanför SWAMID
 - cocov1-1, cocov1-2 - GÉANT CoCo (v1)
 - cocov1-3 - GÉANT CoCo (v1) utanför SWAMID
 - rands - REFEDS R&S

Release-check

- Inga stora förändringar
- Samarbete
 - eduGAIN ?

Shibboleth WebAuthnAuthentication plugin

- Ny plugin som stödjer Web Authentication API (WebAuthn) som en del av FIDO2-standarden, vilket möjliggör FIDO2-autentisering
- Detta möjliggör stark autentisering av användare med hjälp av offentliga nycklar
 - med andra ord – passkeys!
- Första version (1.0.0) släpptes i december 2024
- En ny version (1.1.0) släpptes i mars 2025 efter testning och feedback från SWAMID operations

Autentisering på flera sätt

- som en singelfaktor inom en bredare MFA-lösning
- som en ensam-faktor där användarnamnet anges av användaren (passwordless)
- som en ensam-faktor där användarnamnet inte anges av användaren men istället identifieras implicit från den valda FIDO2 credential (usernameless)

Features

- Administration flöde för användarna
 - så att en användare kan skapa och hantera sina egna credentials
- Management flöde för administratörer
 - så att en administratör kan hantera andras credentials
- Metadata
 - systemet stödjer läsning av metadata för authenticators från bl.a. FIDO alliance metadata service
- Credential registration policies
 - tillåter styrning av vilka typer av authenticators man vill tillåta (t.ex. endast hårdvara säkerhetsnycklar)

SWAMID testning

- Ett MFA authn flöde i second factor mode med lösenord först och sedan en FIDO2 credential (passkey på en Yubikey)
- Tillåter självregistrering av en credential med endast lösenord
- Kräver MFA (lösenord + credential) för att hantera registrerade credentials
- Kan fungera som en multifaktor på AL2-nivå

Video – WebAuthn demo (2 min)

- 00:00 - Användaren testemp1 skapar sin första credential (på en Yubikey) efter inloggning med sitt lösenord.
- 00:28 - Användaren testemp1 testar MFA-inloggning på release-check. Loggar in med lösenord + Yubikey.
- 01:10 - Användaren testemp1 hanterar sina credentials. Observera att användaren måste göra en MFA-inloggning eftersom en credential är redan registrerad.
- 01:27 – Admin-användare testemp3 (som redan har sin egen credential) loggar in i management-gränssnittet och tar bort den credential för användaren testemp1.



Please enter your username below.

KauID

Next

▪ [Need Help?](#)

KARLSTADS UNIVERSITET 651 88 Karlstad



Mer information

- Shibboleth wiki
 - <https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/3395125387/WebAuthn>
- Webinar
 -

ADFS Toolkit

- Ny version, 2.3.0
<https://github.com/fedtools/adfstoolkit>
- Nytt sätt att uppgradera
Update-ADFSTk
- Dokumentationen har uppdaterats på SWAMID:s wiki
<https://wiki.swamid.se>
- Stöd för f-ticks

F-ticks – f-ticks.edugain.org

Authentications processed by the IdP



ADFS Toolkit - tips

- Ha en testmiljö (skild från produktionsmiljön) ;)
- Kör entitetstestaren

```
$ReleaseCheckSPs = Get-ADFSTkToolEntityId -Search release-check.swamid.se | Select -ExpandProperty Identifier
```

```
$i = 0
```

```
foreach ($ReleaseCheckSP in $ReleaseCheckSPs) {
```

```
    $i++
```

```
    Write-Host "Importing '$ReleaseCheckSP'... ($i/$($ReleaseCheckSPs.Count))" -ForegroundColor Yellow
```

```
    Import-ADFSTkMetadata -ConfigFile C:\ADFSToolkit\config\institution\config.Swamid.xml -EntityId  
    $ReleaseCheckSP -ForceUpdate
```

```
}
```



SWAMID

Swedish Academic Identity Federation

Frågor?



SWAMID

Swedish Academic Identity Federation