ADFS-integraatio

MPASSid lisätään ADFS:ään PowerShell komentojen avulla. Alla esimerkki Powershell-komennot, joilla MPASSid lisätään ADFS:ään. Komennoista on kaksi versiota riippuen siitä, että luetaanko MPASSid:n metadata internetin kautta vai paikallisesta kopiosta.

MPASSid:n lisääminen ADFS:ään

MPASSid:n metadata url-osoitteella

```
$name = "mpass-proxy"
$metadataUrl = "https://mpass-proxy.csc.fi/Shibboleth.sso/Metadata"

Add-ADFSRelyingPartyTrust -MetadataUrl $metadataUrl -Name $name -AutoUpdateEnabled $true -EncryptClaims $true -
SignedSamlRequestsRequired $true -EncryptionCertificateRevocationCheck none  -SigningCertificateRevocationCheck none
```

MPASSid:n metadata paikallisesti

Kopioi ensin MPASSid:n metadata ADFS-palvelimelle haluamaasi hakemistoon mpass-proxy-metadata.xml nimellä.

Päivitä alla oleviin komentoihin metadatatiedoston sijainti ja nimi, jos käytit jotain toista tiedostonimeä.

```
$name = "mpass-proxy"
$metadataFile = "c:\<hakemisto>\mpass-proxy-metadata.xml"

Add-ADFSRelyingPartyTrust -MetadataFile $metadataFile -Name $name -EncryptClaims $true -SignedSamlRequestsRequired $t
rue -EncryptionCertificateRevocationCheck none  -SigningCertificateRevocationCheck none


# MPASSid:n tiedot voi päivittää metadatasta komennolla
Update-AdfsRelyingPartyTrust -TargetName $name -MetadataFile $metadataFile
```

MPASSid:lle lähetettävien attribuuttien määrittely

ADFS:lle määritellään claim rulejen avulla mitä attribuutteja käyttäjästä välitetään palveluun kirjautumisen yhteydessä. Tarvittavat määritykset voi tehdä joko Powershell-komennoilla, kopioimalla ja tarvittaessa muokkaamalla tämän ohjeen esimerkki claim ruleja tai määrittämällä ne ADFS:n hallintakonsolista. Löydät tarkemmin tietoa claim ruleista tämän ohjeen **Claim Rulet** kohdasta.

Päivitä alla oleviin komentoihin MPASSid:lle lähetettäviä attribuutteja vastaavat AD:n attribuutit. Types kohdassa määritellään minkä tyyppisenä attribuutit lähetetään MPASSid:lle ja query kohdassa määritellään mistä AD:n attribuutista vastaava attribuutti löytyy. Types ja query kohtien attribuuttien järjestys vastaa toisiaan.

MPASSid:n claim rulejen määritys

```
$issuanceTransformRules = '@RuleName = "Send MPASSid Attributes"c:[Type == "http://schemas.microsoft.com/ws/2008
/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("mpassUserIdentity", "mpassGivenName", "mpassSurname", "mpassAccountName", "mpassLearnerId",
"mpassSchoolCode", "mpassClassLevel", "mpassClassCode", "mpassUserRole", "mpassLearningMaterialsCharge","
mpassNickName"), query = ";objectGuiD,givenName,sn,userPrincipalName,<learnerId>,<schoolCode>,<classLevel>,
<classCode>,<userRole>,<learningMaterialsCharge>,<nickName>;{0}", param = c.Value);';

$issuanceAuthorizationRules = '@RuleTemplate = "AllowAllAuthzRule" => issue(Type = "http://schemas.microsoft.com
/authorization/claims/permit", Value = "true");'

$name = "mpass-proxy"

Set-ADFSRelyingPartyTrust -TargetName $name -IssuanceAuthorizationRules $issuanceAuthorizationRules -
IssuanceTransformRules $issuanceTransformRules
```

Huom! `mpassAccountName` ei ole pakollinen uusissa adfs-integraatioissa. Sen voi myös poistaa vanhoista, jos asiasta sovitaan ensin MPASSid tuen kanssa.

Useamman koulukoodin lähettäminen ja muut moniarvoiset attribuutit

Jos oppilailla tai opettajilla on useita kouluja, voit välittää koulukoodit mpassSchoolCode attribuutissa puolipistein eroteltuna.

Tarkemmat ohjeet moniarvoisten attribuuttien välittämisestä MPASSid:llä löytyy täältä.

ADFS:n tiedot MPASSid:lle

ADFS:n tiedot pitää lisätä MPASSid:lle ennen kuin kirjautuminen toimii. Lisääminen tapahtuu ADFS:n metadatan avulla. Metadata löytyy oletuksen ADFS-palvelimelta osoitteesta https://<palvelimen_nimi>/FederationMetadata/2007-06/FederationMetadata.xml. Lähetä ADFS:n metadata osoitteeseen mpass@oph.fi.

Claim Rulet

Alla esimerkki claim rule määrityksiä. Näitä voi kopioida ja liittää ADFS:n Relying Partyn määrityksiin ADFS:n hallintakonsolista. Määrityksiin pitää muokata mistä AD:n attribuutista MPASSid:lle lähetettävä attribuutti löytyy.

- Claim rule tekee kyselyn AD:lle ja hakee kyselyssä määritellyt attribuutit
- Types -kohdassa on määritelty minkä tyyppisinä attribuutit lähetetään MPASSid:lle ja query kohdassa on määritelty mistä AD:n attribuutista haluttu tieto löytyy.
- Types ja query kohtien järjestys vastaa toisiaan. Eli esimerkiksi mpassUserIdentity attribuutti haetaan AD:n objectGuid attribuutista.
- Voit lisätä, muuttaa ja poistaa attribuutteja tarvittessa (Tietomallissa pakollisia attribuutteja ei voi poistaa).

```
Send MPASSid Attributes
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"]
 => issue(store = "Active Directory", types = ("mpassUserIdentity", "mpassAccountName", "mpassGivenName", "mpass
Surname",  "mpassLearnerId", "mpassSchoolCode", "mpassClassLevel", "mpassClassCode", "mpassUserRole",
"mpassLearningMaterialsCharge","mpassNickName"), query = ";objectGuiD,userPrincipalName,givenName,sn,
<learnerId>,<schoolCode>,<classLevel>,<classCode>,<userRole>,<learningMaterialsCharge>,<nickName>;{0}", param
= c.Value);
```

Huom! `mpassAccountName` ei ole pakollinen uusissa adfs-integraatioissa. Sen voi myös poistaa vanhoista, jos asiasta sovitaan ensin MPASSid tuen kanssa.

Esimerkkejä erilaisista claim ruleista

Jos määrittelet MPASSid:lle lähetettäviä attribuutteja erillisillä claim ruleilla, niin varmista ettei niitä lähetä myös jossain toisessa attribuutissa.

Maksullisuusattribuutin lähettäminen kiinteänä arvona

```
Send mpassLearningMaterialsCharge
=> issue(Type = "mpassLearningMaterialsCharge", Value = "1");
```

Numeerisen roolitiedon muuttaminen tekstimuotoiseksi

```
# Haetaan käyttäjän rooli AD:n employeeType attribuutista ja lisätään (add) se käyttäjän attribuutteihin
Add Employee Type as Role
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"]
 => add(store = "Active Directory", types = ("http://schemas.microsoft.com/ws/2008/06/identity/claims/role"),
query = ";employeeType;{0}", param = c.Value);

# Tutkitaan roolin arvo ja lähetetään eteenpäin (issue) arvoa vastaava tekstimuotoinen rooli
Send mpassUserRole oppilas
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/role", Value =~ "^1" ]
 => issue(Type = "mpassUserRole", Value = "oppilas");

Send mpassUserRole opettaja
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/role", Value =~ "^2" ]
 => issue(Type = "mpassUserRole", Value = "opettaja");
```

Roolitiedon lähettäminen OU-rakenteen mukaan.

Tätä voi hyödyntää mikäli opettajat ja oppilaat ovat omissa OU:issaan, eikä heidän käyttäjäobjekteissa ole roolitietoa missään attribuutissa.

```
# Ensimmäinen claim rule - haetaan käyttäjän distinguishedName ja asetetaan se claim:distinguishedName -
claimiin.
# Tämä claimia ei lähetetä ADFS:stä eteenpäin (=> add() vs => issue()).
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"]
=> add(store = "Active Directory", types = ("claim:distinguishedName"), query = ";distinguishedName;{0}", param
= c.Value);

# Toinen claim rule, jossa tutkitaan sisälsikö claim OU=Oppilaat tekstin. Ja mikäli sisälsi, niin palautetaan
mpassUserRole:na Oppilas.
c:[Type == "claim:distinguishedName", Value =~ "(OU=Oppilaat)"]
=> issue(Type = "mpassUserRole", Value = "Oppilas");

# Kolmas claim rule, jossa tutkitaan sisälsikö claim OU=Opettajat tekstin. Ja mikäli sisälsi, niin palautetaan
mpassUserRole:na Opettaja.
c:[Type == "claim:distinguishedName", Value =~ "(OU=Opettajat)"]
=> issue(Type = "mpassUserRole", Value = "Opettaja");
```

Windows Server 2019 ADFS

Windows Server 2019 ADFS lisää oletuksena metadataansa contact personin email addressin tyhjänä elementtinä. Jotta metadatan validointi toimii, niin email address tulee olla määriteltynä.

Samalla kannattaa varmistaa ettei metadatassa ole contact personissa muitakaan tyhjiä elementtejä.

```
# Tarkista ensin onko contact person:n tiedot jo annettu:
(Get-AdfsProperties).ContactPerson

# Jos edellisen komennon tuloksena EmailAddresses on tyhjä, niin tällä voit lisätä sen.
# Huom! tämä ylikirjoittaa mahdolliset aiemmat ContactPerson määritykset, joten kaikki tiedot tulee asettaa
uudelleen.
$CP = New-AdfsContactPerson [-Company <string>] [-EmailAddress <string[]>] [-GivenName <string>] [-
TelephoneNumber <string[]>] [-Surname <string>]
Set-AdfsProperties -ContactPerson $CP
```

OPH:lle toimitettavat tiedot integraatiotyypistä riippumatta

MPASSid-integraation rakentamista varten jokaisen koulutustoimijan on ilmoitettava seuraavat tiedot palveluosoitteeseemme **mpass(at)oph.fi .**

1. Oppilaitostyypit, joilla aiotte MPASSid:tä käyttää. Hyväksytyt oppilaitostyypit koodiarvoineen löytyvät täältä: https://koski.opintopolku.fi/koski/dokumentaatio/koodisto/oppilaitostyyppi/latest
2. Kunnan/koulutustoimijan logotiedoston, jonka haluatte näytettävän MPASSid:n koulunvalintasivulla.
    - Logo: png-muodossa, koko 125x36 px.

Kun nämä tiedot on lähetetty MPASSid:lle ja liittymissopimukset ovat allekirjoitettuna molempien osapuolten toimesta, saadaan integraatio päälle usein parin arkipäivän kuluessa.