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 rslejen 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", "mpassCryptID",
"mpassMunicipalityCode", "mpassSchoolCode", "mpassClassLevel", "mpassClassCode", "mpassUserRole"), query = ";
objectGuiD,givenName,sn,userPrincipalName,<cryptID>,<municipalityCode>,<schoolCode>,<classLevel>,<classCode>,
<userRole>;{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
```

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 tuki@mpass.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. Jos esimerkiksi käyttäjän tiedoista AD:lla ei löydy kuntakoodia, niin poista types kohdasta "mpassMunicipalityCode" ja query kohdasta vastaava attribuutti.

```
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", "mpassCryptID", "mpassMunicipalityCode", "mpassSchoolCode", "mpassClassLevel", "mpassClassCode", "mpas
sUserRole"), query = ";objectGuiD,userPrincipalName,givenName,sn,<cryptID>,<municipalityCode>,<schoolCode>,
<classLevel>,<classCode>,<userRole>;{0}", param = c.Value);
```

Esimerkkejä erilaisista claim ruleista

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

Kuntakoodin lähettäminen kiinteänä arvona

```
Send mpassMunicipalityCode
=> issue(Type = "mpassMunicipalityCode", Value = "123");
```

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 henklökunta
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/role", Value =~ "^0" ]
 => issue(Type = "mpassUserRole", Value = "henkilökunta");


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");
```