

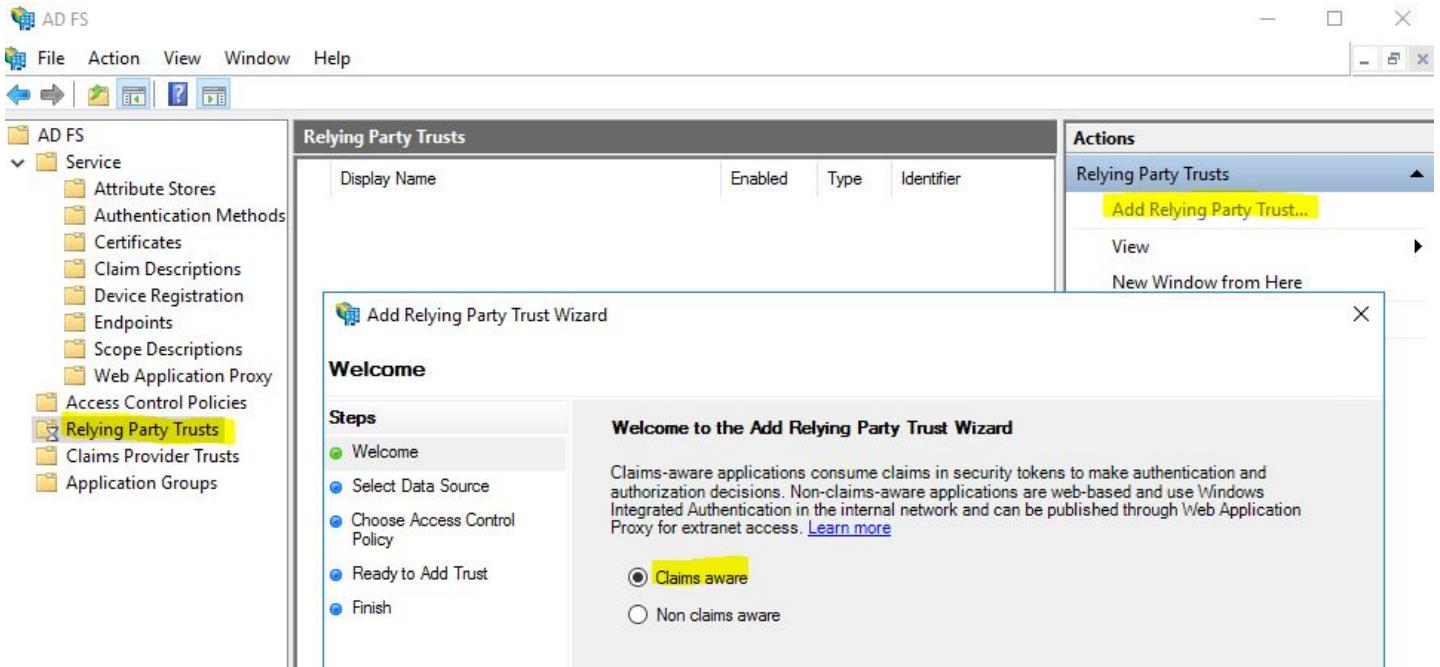
## Configurer ADFS comme fournisseur d'identités SAML pour Publik

On suppose dans ce qui suit qu'un système Publik est installé sur <https://demarches.ville.fr/>. Le système de connexion est alors présent sur <https://connexion.demarches.ville.fr/> et c'est lui qui doit être référencé comme « Service Provider » dans ADFS.

### Ajout du « Relying Party » dans ADFS

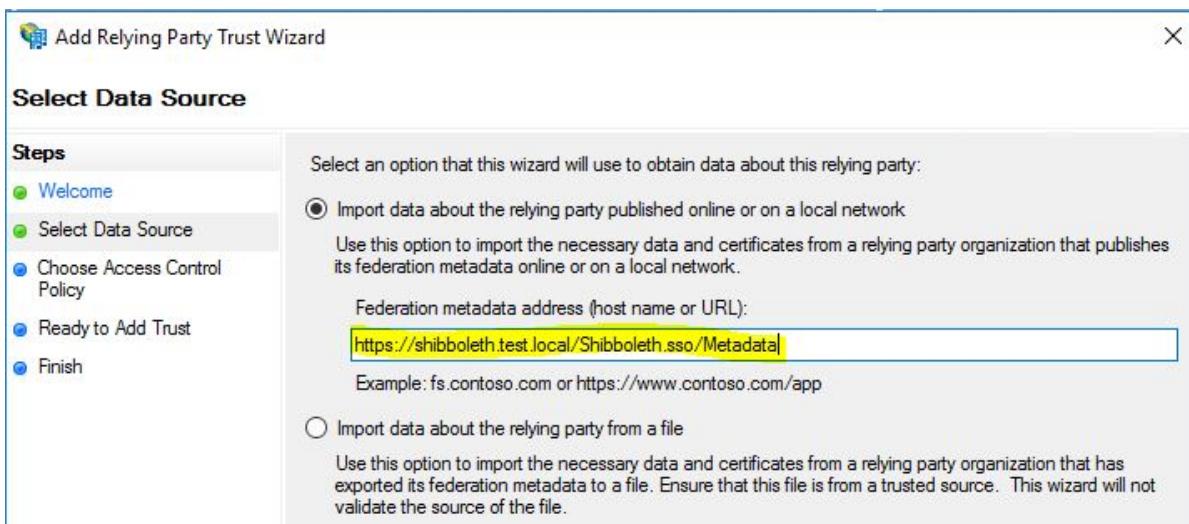
La configuration des services ADFS s'effectue via la console « AD FS Management ». Nous créons « relying party trust » à partir des informations présentes dans les métadonnées SAML 2.0 de Publik.

En cliquant sur « Add Relying Party Trust... » on sélectionne le type d'application souhaitée: Claim aware.



Nous allons à présent utiliser la fonction d'import automatique de la configuration Publik présente dans les métadonnées.

**L'URL des métadonnées de Publik est de la forme <https://connexion.demarches.ville.fr/accounts/saml/metadata/>** (à indiquer dans la partie en jaune de la copie d'écran ci-dessous)



Saisir le nom du « Relying Party Trust: », indiquer par exemple **connexion.demarches.ville.fr**

## Add Relying Party Trust Wizard

### Specify Display Name

<b>Steps</b>	Enter the display name and any optional notes for this relying party.
<span style="color: green;">●</span> Welcome	Display name:
<span style="color: green;">●</span> Select Data Source	<input type="text" value="shibboleth.test.local"/>
<span style="color: green;">●</span> Specify Display Name	Notes:
<span style="color: blue;">●</span> Choose Access Control Policy	
<span style="color: blue;">●</span> Ready to Add Trust	
<span style="color: blue;">●</span> Finish	

On choisit ensuite qui aura accès à Publik via ADFS, cela dépend des choix de la collectivité, dans un premier temps choisir **everyone** (tout le monde) simplifie la configuration

## Add Relying Party Trust Wizard

### Choose Access Control Policy

<b>Steps</b>	Choose an access control policy:																		
<span style="color: green;">●</span> Welcome	<table border="1"><thead><tr><th>Name</th><th>Description</th></tr></thead><tbody><tr><td>Permit everyone</td><td>Grant access to everyone.</td></tr><tr><td>Permit everyone and require MFA</td><td>Grant access to everyone and requir...</td></tr><tr><td>Permit everyone and require MFA for specific group</td><td>Grant access to everyone and requir...</td></tr><tr><td>Permit everyone and require MFA from extranet access</td><td>Grant access to the intranet users ar...</td></tr><tr><td>Permit everyone and require MFA from unauthenticated devices</td><td>Grant access to everyone and requir...</td></tr><tr><td>Permit everyone and require MFA, allow automatic device registr...</td><td>Grant access to everyone and requir...</td></tr><tr><td>Permit everyone for intranet access</td><td>Grant access to the intranet users.</td></tr><tr><td>Permit specific group</td><td>Grant access to users of one or more...</td></tr></tbody></table>	Name	Description	Permit everyone	Grant access to everyone.	Permit everyone and require MFA	Grant access to everyone and requir...	Permit everyone and require MFA for specific group	Grant access to everyone and requir...	Permit everyone and require MFA from extranet access	Grant access to the intranet users ar...	Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir...	Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir...	Permit everyone for intranet access	Grant access to the intranet users.	Permit specific group	Grant access to users of one or more...
Name	Description																		
Permit everyone	Grant access to everyone.																		
Permit everyone and require MFA	Grant access to everyone and requir...																		
Permit everyone and require MFA for specific group	Grant access to everyone and requir...																		
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar...																		
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir...																		
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir...																		
Permit everyone for intranet access	Grant access to the intranet users.																		
Permit specific group	Grant access to users of one or more...																		
<span style="color: green;">●</span> Select Data Source																			
<span style="color: green;">●</span> Specify Display Name																			
<span style="color: green;">●</span> Choose Access Control Policy																			
<span style="color: blue;">●</span> Ready to Add Trust																			
<span style="color: blue;">●</span> Finish																			

Avant de valider la fin de la configuration, nous allons vérifier que le « Relying party identifier » et bien identique à « ApplicationDefaults EntityID » de Publik :

## Add Relying Party Trust Wizard

<b>Steps</b>	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.
<span style="color: green;">●</span> Welcome	
<span style="color: green;">●</span> Select Data Source	
<span style="color: green;">●</span> Specify Display Name	
<span style="color: green;">●</span> Choose Access Control Policy	
<span style="color: green;">●</span> Ready to Add Trust	
<span style="color: blue;">●</span> Finish	

Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Notes

Specify the display name and identifiers for this relying party trust.

Display name:

Relying party identifiers:

Nous laisserons la case « Configure claims issuance policy for this application » cochée. La fenêtre nous permettant d'éditer le contenu de notre claim s'ouvre.

**Finish****Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

The relying party trust was successfully added.

 Configure claims issuance policy for this application**Configuration des attributs à envoyer à Publik (*claims*)**

Dans la liste des « Relying Party Trusts » s'affiche désormais celui de Publik qui vient d'être ajouté. Cliquer dessus et choisir l'**action « Edit Claim Issuance Policy... »**

Le bouton « Add Rules » permet alors de définir les attributs à envoyer.

Dans le cadre d'une connexion à Publik il faut envoyer les attributs suivants :

- Name (<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>)
- Givenname (<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname>, le prénom)
- Surname (<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname>, le nom)
- Emailaddress (<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>, l'adresse email)

**Attention** : La copie d'écran ci-dessous est un exemple qui montre la configuration avec l'envoi de UPN et Display Name ; mais c'est Name, GivenName, Surname et EmailAddress qui devront apparaître dans le cas d'un Publik.

**Configure Rule****Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

UPN &amp; DisplayName

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	UPN
Display-Name	Name
*	

**Configuration côté Publik**

La configuration du « Relying Party Trust ADFS » est alors présent terminée sur ADFS, qui reconnaît désormais Publik comme service de confiance.

Il faut maintenant configurer Publik pour qu'il utiliser ADFS comme source d'identité possible (en plus des comptes locaux et du connexion FranceConnect éventuelle).

**Cas AD "On premise" - hébergé par la collectivité**

Pour cela, et si ce n'est pas déjà fait, il faut communiquer à Entr'ouvert l'adresse des métadonnées de l'IdP ADFS SAML, qui est normalement de la forme <https://idp.ville.fr/FederationMetadata/2007-06/FederationMetadata.xml> (où idp.ville.fr est le nom du

serveur ADFS sur Internet).

A toutes fins utiles (surtout en interne pour Entr'ouvert), voici la procédure pour la configuration dans Publik.

#### 1. Création de clés 2048 bits :

```
openssl req -x509 -sha256 -newkey rsa:2048 -nodes -keyout sp-saml.key -out sp-saml.crt -batch -subj '/CN=connexion.demarches.ville.fr' -days 3652
```

#### 2. Copier les fichiers sp-saml.key et sp-saml.crt dans le répertoire du tenant

/var/lib/authentic2-multitenant/tenants/connexion.demarches.ville.fr/

#### 3. Créer un rôle "Connexion ADFS"

#### 4. Obtenir l'URL des métadonnées, comme dit plus haut de la forme

"<https://idp.ville.fr/FederationMetadata/2007-06/FederationMetadata.xml>" et la mettre dans settings.json (voir plus bas) pour la clé METADATA\_URL

#### 5. Ajouter dans settings.json :

```
{
  "A2_AUTH_SAML_ENABLE": true,
  "MELLON_PUBLIC_KEYS": [
    "/var/lib/authentic2-multitenant/tenants/connexion.demarches.ville.fr/sp-saml.crt"],
  "MELLON_PRIVATE_KEY": [
    "/var/lib/authentic2-multitenant/tenants/connexion.demarches.ville.fr/sp-saml.key"],
  "MELLON_PROVISION": true,
  "MELLON_IDENTITY_PROVIDERS": [
    {
      "METADATA_URL": "https://idp.ville.fr/FederationMetadata/2007-06/FederationMetadata.xml",
      "PROVISION": true,
      "A2_ATTRIBUTE_MAPPING": [
        {"action": "rename", "from": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname", "to": "givenname"},
        {"action": "rename", "from": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname", "to": "surname"},
        {"action": "rename", "from": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name", "to": "name"},
        {"action": "rename", "from": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress", "to": "email"},
        {"attribute": "first_name", "saml_attribute": "givenname", "mandatory": true},
        {"attribute": "last_name", "saml_attribute": "surname", "mandatory": true},
        {"attribute": "username", "saml_attribute": "name", "mandatory": true},
        {"attribute": "email", "saml_attribute": "email", "mandatory": true},
        {"action": "toggle-role", "role": {"name": "Connexion ADFS"}}
      ],
      "LOOKUP_BY_ATTRIBUTES": [
        {"saml_attribute": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress", "user_field": "email"}
      ]
    }
  ]
}
```

#### Cas où l'IdP n'est pas accessible depuis Authentic

Dans ce cas les métadonnées ne pourront pas être téléchargées par authentic, on modifie donc les étape 4 et 5:

#### 4. Demander les métadonnées de l'ADFS et les copier dans

/var/lib/authentic2-multitenant/tenants/connexion.demarches.ville.fr/adfs-metadata.xml

#### 5. Retirer la clé METADATA\_URL de la configuration et mettre à la place "METADATA":

"/var/lib/authentic2-multitenant/tenants/connexion.demarches.ville.fr/adfs-metadata.xml",

#### Cas Azure AD "SaaS" - hébergé par Microsoft

La configuration est quasiment la même mais on ne peut pas facilement deviner l'URL des métadonnées, car elle est unique pour chaque fournisseur de service et généralement de la forme suivante :

<https://login.microsoftonline.com/180627ee-80c9-4bec-95e6-81b5fec81ff/federationmetadata/2007-06/>

Par contre elle est toujours accessible publiquement et donc la configuration via un fichier ne sera normalement jamais nécessaire. Il est important de passer par une URL car les clés pourraient être souvent mises à jour.

## Fichiers

shibboleth-sp-3-avec-iis-10-et-php-img16.jpg	58,1 ko	18 décembre 2019	Thomas Noël
shibboleth-sp-3-avec-iis-10-et-php-img15.jpg	51,1 ko	18 décembre 2019	Thomas Noël
shibboleth-sp-3-avec-iis-10-et-php-img14.jpg	23,3 ko	18 décembre 2019	Thomas Noël
shibboleth-sp-3-avec-iis-10-et-php-img17.jpg	41,4 ko	18 décembre 2019	Thomas Noël
shibboleth-sp-3-avec-iis-10-et-php-img13.jpg	52,7 ko	18 décembre 2019	Thomas Noël
shibboleth-sp-3-avec-iis-10-et-php-img12.jpg	30,7 ko	18 décembre 2019	Thomas Noël
Shibboleth-sp-3-avec-iis-10-et-php-img11.jpg	55,9 ko	18 décembre 2019	Thomas Noël
shibboleth-sp-3-avec-iis-10-et-php-img10.jpg	73,7 ko	18 décembre 2019	Thomas Noël