Authentic 2 - Bug #45200

Gestion par l'usager de ses consentements sur le SSO et et les scopes de diffusion d'attributs

16 juillet 2020 18:16 - Nicolas Roche

Statut:	Fermé	**Début:**	16 juillet 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Nicolas Roche	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Sur la page Mon compte, l'usager doit pouvoir retrouver les consentements horodatés donnés à chaque partenaire et doit pouvoir les supprimer.
(ticket client #21966)

Demandes liées:

Lié à Intégrations graphiques Publik - Development #45496: Gestion par l'usag...	**Fermé**	**27 juillet 2020**
Lié à Authentic 2 - Development #46182: En BO, gestion des consentements de l...	**Fermé**	**28 août 2020**

Révisions associées

Révision 1a3bd4bb - 29 juillet 2020 09:45 - Nicolas Roche

profile_views: add a profil page to manage authorized oauth services (#45200)

Historique

#2 - 16 juillet 2020 18:18 - Nicolas Roche

- Fichier 0001-oidc-revoke-oidc-claims-authorization-21966.patch ajouté

- Tracker changé de Support à Bug

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Pour info (critiques, conseils...), je pense partir sur ce patch, puis écrire le gabarit dans

- authentic/src/authentic2/templates/authentic2/accounts.html et
- publik-base-theme/templates/authentic2/accounts.htm

```
...
{% for authorization in oidc_authorizations %}
      <tr>
        <td>{{ authorization.client }}</td>
        <td>{{ authorization.scopes }}</td>
        <td>{{ authorization.created }}</td>
        <td>{{ authorization.expired }}</td>
        <td><a class="icon-remove" href="{% url 'oidc-unconsent' authorization.id %}"></a></td>
      </tr>
```

#3 - 16 juillet 2020 18:22 - Nicolas Roche

- Statut changé de Solution proposée à En cours

#4 - 16 juillet 2020 18:57 - Frédéric Péters

- Fichier revoke-oauth-app.png ajouté

Il est écrit "Sur la page Mon compte" mais je l'interpréterais bien comme "Depuis la page Mon compte", en imaginant ainsi ne pas charger d'informations supplémentaires cette page.

De là donc j'imagine une nouvelle page, qui liste les services autorisés, et pour chacun la possibilité de révoquer l'autorisation.

Cela dans authentic, sans aller ensuite faire marcher la chose par du code de gabarit dans publik-base-theme.

Pour cette page, je regarderais ce qui se fait, par exemple pour la gestion des autorisations accordées à un compte github capture attachée; en interprétant ça on peut imaginer cette maquette :

```
Gestion des consentements
-------------------------

Vous avez autorisé la diffusion de votre profil à 3 services.

# Titre du service 1                              [ Retirer l'autorisation ]
# Autorisation : 4 janvier 2020 / Dernière connexion : 12 avril 2020

# Titre du service 2                              [ Retirer l'autorisation ]
# Autorisation : 4 janvier 2020 / Dernière connexion : 12 avril 2020

# Titre du service 3                              [ Retirer l'autorisation ]
# Autorisation : 4 janvier 2020 / Dernière connexion : 12 avril 2020
```

(je ne sais pas si on a l'info de dates d'autorisation et dernière connexion, faire sans et attendre le journal des actions de l'usager pour ajouter ça).

(et par rapport au bout qui est dans le patch, la possibilité de retirer un consentement ça doit être un POST vers le serveur, pas un GET).

#5 - 17 juillet 2020 17:22 - Nicolas Roche

- Fichier Screenshot_2020-07-17 Portail - Connexion.png ajouté

- Fichier 0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch ajouté

J'ai fais de mon mieux pour suivre les conseils mais j'ai le sentiment d'être tombé à côté,
ne serais-ce que parce que mon rendu est super moche.

#6 - 17 juillet 2020 17:28 - Benjamin Dauvergne

- mettre l'URL sous accounts, dans /accounts/authorizations/
- login_required() on l'applique plutôt à l'objet retourné par .as_view()
- ne pas mettre les scopes tant qu'on ne sait pas les afficher mieux que sous forme de code
- il doit manquer des choses dans le template de ProfileView, pourquoi y passer les autorisations ? Tout ce qui est dans ProfileView doit être conditionné par la présence effective et l'activation de l'application authentic2_idp_oidc (on ne sais jamais si on la désactive on ne souhaite pas que la vue pète), le plus simple serait que ça s'autoconfigure via des hooks mais c'est pas urgent.

#7 - 17 juillet 2020 17:30 - Frédéric Péters

Pas de tableaux c'est de fait directement moche. Pas le "revoke all" qui ne m'a pas semblé être demandé. Pas de <input type=submit> pour faire des boutons.

#8 - 20 juillet 2020 15:22 - Nicolas Roche

- Fichier Screenshot_2020-07-20 Authentic2 - alone dev publik love(1).png ajouté

- Fichier Screenshot_2020-07-20 Authentic2 - alone dev publik love.png ajouté

- Fichier 0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch ajouté

Remarques prises en compte :

- URL sous accounts, dans /accounts/authorizations/ (du coup j'ai déplacé le code dans src/authentic2/views.py)
- login_required() appliqué à l'objet retourné par .as_view()
- ne pas mettre les scopes tant qu'on ne sait pas les afficher mieux que sous forme de code
- ProfileView, pourquoi y passer les autorisations ? (oups, j'ai mal nettoyé mon précédent patch)
- Présentation sous forme de listes
- Pas de "revoke all"
- <button> sur les formulaires
- captures d'écran avec un authentic standalone (précédemment c'était sur un devinst avec le thème de saint-denis)

Je ne suis pas à l'aise avec les aspects graphiques (qui s'appliquent à la fois sur un authentique seul et sur Publik) et je suis à l'écoute de vos propositions. Je pourrais par exemple faire un unique formulaire avec des cases à cocher pour supprimer les autorisations à supprimer... ou pas.

#9 - 20 juillet 2020 15:35 - Frédéric Péters

Il manque nettement un titre, qui peut être "Gestion des consentements". (comme dans ma "maquette")

Je n'appellerais pas ça "applications" mais "services". (comme dans ma "maquette")

(pareil pour les apps dans les noms de vues/url/blocs/etc.)

Je n'écrirais pas "Delete", qui va nécessairement se trouver traduit en "Supprimer", alors qu'on préférera "Retirer". (comme dans ma "maquette").

Il me semble utile d'inclure un autour de la ligne des informations de date, pour permettre la maquette.

Il manque les appels {% trans ... %} dans le gabarit.

Et j'aurais comme texte là-dessous, si ce sont les infos qu'on a, "Date d'autorisation: ... / Expiration: ...".

"You have no granted" → no*T* granted.

J'anticiperais GLC et mettrais a minimal un bloc d'extension au début du formulaire (pour dans le gabarit particulier il puisse être inséré là le nécessaire pour reprendre le logo).

#10 - 20 juillet 2020 17:25 - Nicolas Roche

- Fichier Screenshot_2020-07-20 Portail - Connexion(1).png ajouté

Remarques prises en compte (merci).

- Il manque nettement un titre, qui peut être "Gestion des consentements". (comme dans ma "maquette")
  Le titre ne s'affiche pas dans authentiqocks top/bottom ue "standalone" (voir par exemple sur la page d'édition du profile : accounts/edit/)
  (du coup je pose une capture d'écran prise depuis mon publik-devinst)
  J'ai mis "Consent Management" (j'ai hésité avec "Granted Services").

- Je n'appellerais pas ça "applications" mais "services". (comme dans ma "maquette")
  (pareil pour les apps dans les noms de vues/url/blocs/etc.)
  oui, et j'en ai profité pour préfixer le nom du template par "accounts_" pour refléter l'url associée ("accounts_authorizations/")

- Je n'écrirais pas "Delete", qui va nécessairement se trouver traduit en "Supprimer", alors qu'on préférera "Retirer". (comme dans ma "maquette").
  => Revoke

- Il me semble utile d'inclure un autour de la ligne des informations de date, pour permettre la maquette.

- Il manque les appels {% trans ... %} dans le gabarit.
  A ce propos, j'ai remis l'indication sur le nombre de services authorisés donnée dans la maquette.
  (et j'ai insérés ces informations dans le bloc "top")

- Et j'aurais comme texte là-dessous, si ce sont les infos qu'on a, "Date d'autorisation: ... / Expiration: ...".
- "You have no granted" → no*T* granted.

- J'anticiperais GLC et mettrais a minimal un bloc d'extension au début du formulaire (pour dans le gabarit particulier il puisse être inséré là le nécessaire pour reprendre le logo).
  J'ai ajouté 2 blocs (top et bottom) à l'intérieur de la boucle (avec le nom de la classe au singulier)

#11 - 20 juillet 2020 17:31 - Frédéric Péters

> A ce propos, j'ai remis l'indication sur le nombre de services authorisés donnée dans la maquette.

Faut gérer correctement singulier/pluriel ({% blocktranslate } avec { plural %} dedans, cf https://docs.djangoproject.com/en/dev/topics/i18n/translation/#std:templatetag-blocktranslate)

> Il me semble utile d'inclure un autour de la ligne des informations de date, pour permettre la maquette.

Mal compris, le propos était d'avoir dans un span englobant ce qui apparait sur la seconde ligne de la maquette, i.e. autour de l'ensemble du texte qui donne les dates.

```
+       {% trans "/ Expire on: " %}
```

Le / n'est pas à marquer pour traduction, ni à inclure dans ce span, tape le entre les deux.

#12 - 20 juillet 2020 18:17 - Nicolas Roche

- Fichier 0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch ajouté

- Statut changé de En cours à Solution proposée

Remarques prises en compte :

- Faut gérer correctement singulier/pluriel ({% blocktranslate } avec { plural %} dedans
- Il me semble utile d'inclure un autour de la ligne des informations de date, pour permettre la maquette.
  (j'ai laissé le juste autour des dates)
- Le / n'est pas à marquer pour traduction, ni à inclure dans ce span, tape le entre les deux.

#13 - 25 juillet 2020 11:27 - Frédéric Péters

- Fichier accounts_authorized_oauth_services.html ajouté

- Fichier Screenshot_2020-07-25 Authentic.png ajouté

Sur le fond je pense qu'il y a peut-être une différence de perspective qui se révèle dans le sujet du commit, "idp_oidc: revoke oidc claims authorization", là où le ticket est "gestion des consentements", et cette tension se retrouve dans le code, avec le code qui n'est pas sous idp_oidc, mais le code qui y est spécifique, la vue dont la classe s'appelle AuthorizedOauthServicesView mais dont le titre est "Consent Management", etc.

De là je dis que plus ou moins rapidement il y aura volonté de repasser là-dessus pour remettre un peu d'ordre.

Mais je vais pas me mêler de ça davantage.

Il manque à mon sens un paramètre comme,

```
    'allow_account_deletion': app_settings.A2_REGISTRATION_CAN_DELETE_ACCOUNT
```

qui servira pour le gabarit templates/authentic2/accounts.html, genre :

```
...
+      {% if has_authorization_management %}
+        <p><a href="{% url 'authorized-oauth-services' %}">{% trans "Manage service authorizations" %}</a></p
>
+      {% endif %}
       {% if allow_account_deletion %}
         <p><a href="{% url 'delete_account' %}">{% trans "Delete account" %}</a></p>
...
```

Ensuite, sur la page, "inclure un autour de la ligne des informations de date" est encore passé à côté de l'objectif (le oidc-authorized-oauth-service-dates contenant uniquement le "allowed since: ..." et pas l'autre date). Comme mon but était de taper un peu de CSS dans publik-base-theme pour le rendu, j'ai fait le tas de modifications nécessaires et+ à ce fichier, attaché, pour au final permettre le rendu de la capture.

#14 - 27 juillet 2020 16:34 - Nicolas Roche

- Fichier 0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch ajouté

Remarques prises en compte, merci pour l'aide.

#15 - 27 juillet 2020 16:35 - Nicolas Roche

- Lié à Development #45496: Gestion par l'usager de ses consentements sur le SSO et et les scopes de diffusion d'attributs ajouté

#16 - 27 juillet 2020 16:45 - Frédéric Péters

```
A2_REGISTRATION_CAN_MANAGE_SERVICE_AUTHORIZATIONS
```

Le "_REGISTRATION_" doit sauter.

```
    def post(self, request, *args, **kwargs):
        if request.user:
```

Je ne vois pas dans quelle situation ce POST pourrait être appelé sans utilisateur (vu qu'il est décoré login_required).

À part ça, je relis les commentaires passés et de Benjamin il me semble que tu n'as pas répondu à :

> il doit manquer des choses dans le template de ProfileView, pourquoi y passer les autorisations ? Tout ce qui est dans ProfileView doit être conditionné par la présence effective et l'activation de l'application authentic2_idp_oidc (on ne sais jamais si on la désactive on ne souhaite pas que la vue pète), le plus simple serait que ça s'autoconfigure via des hooks mais c'est pas urgent.

De là, pour modérer les changements requis, je dirais que l'affichage du lien devrait être conditionné à la présence de authentic2_idp_oidc (dans INSTALLED_APPS) :

```
+            'allow_authorization_management': app_settings.A2_REGISTRATION_CAN_MANAGE_SERVICE_AUTHORIZATIONS,
```

Aussi, que soit déplacé l'import,

```
+from authentic2_idp_oidc.models import OIDCAuthorization
```

qui foirerait si jamais authentic2_idp_oidc n'était pas activé. (le déplacer dans les méthodes de AuthorizedOauthServicesView).

#17 - 27 juillet 2020 16:46 - Frédéric Péters

Et toujours quand même, taper un meilleur sujet sur le commit.

#18 - 27 juillet 2020 18:42 - Nicolas Roche

- Fichier 0001-profile_views-add-a-profil-page-to-manage-authorized.patch ajouté

Merci pour ces 3 points que j'ai laissé passer.

J'ai mis A2_PROFILE_CAN_MANAGE_SERVICE_AUTHORIZATIONS en ajoutant quand même _PROFILE_ pour me caler sur les autres variables.

Je n'ai pas réussi à tester "en vrai" le cas où l'application authentic2_idp_oidc est désactivée (ça plante avant), mais je pense que c'est couvert par les tests.

Aussi, j'ai modifié le titre du commit et j'ai changé sa catégorie : profile_views.
(Je n'ai pas sorti mon test de test_idp_oidc.py, parce que c'est le seul endroit dans les tests où on utilise les objets OIDCAuthorization.)

#19 - 28 juillet 2020 19:38 - Frédéric Péters

- Statut changé de Solution proposée à Solution validée

Ok, je mettrai un patch sur #45496 dans la foulée.

#20 - 29 juillet 2020 09:46 - Nicolas Roche

- Statut changé de Solution validée à Résolu (à déployer)

```
commit 1a3bd4bb0592900ac7c5aaea45954e8e56fae4be
Author: Nicolas ROCHE <nroche@entrouvert.com>
Date:   Thu Jul 16 17:31:03 2020 +0200

    profile_views: add a profil page to manage authorized oauth services (#45200)
```

#21 - 31 juillet 2020 15:15 - Frédéric Péters

- Statut changé de Résolu (à déployer) à Solution déployée

#22 - 28 août 2020 12:37 - Mikaël Ates (de retour le 29 avril)

- Lié à Development #46182: En BO, gestion des consentements de l'utilisateur donnés lors du SSO OIDC et les scopes de diffusion d'attributs ajouté

Fichiers

0001-oidc-revoke-oidc-claims-authorization-21966.patch	4,87 ko	16 juillet 2020	Nicolas Roche
revoke-oauth-app.png	46,3 ko	16 juillet 2020	Frédéric Péters
Screenshot_2020-07-17 Portail - Connexion.png	23,5 ko	17 juillet 2020	Nicolas Roche
0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch	10,8 ko	17 juillet 2020	Nicolas Roche
Screenshot_2020-07-20 Authentic2 - alone dev publik love(1).png	8,9 ko	20 juillet 2020	Nicolas Roche
Screenshot_2020-07-20 Authentic2 - alone dev publik love.png	21,4 ko	20 juillet 2020	Nicolas Roche
0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch	6,69 ko	20 juillet 2020	Nicolas Roche
Screenshot_2020-07-20 Portail - Connexion(1).png	20,6 ko	20 juillet 2020	Nicolas Roche
0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch	7,86 ko	20 juillet 2020	Nicolas Roche
accounts_authorized_oauth_services.html	2,5 ko	25 juillet 2020	Frédéric Péters
Screenshot_2020-07-25 Authentic.png	26,1 ko	25 juillet 2020	Frédéric Péters
0001-idp_oidc-revoke-oidc-claims-authorization-45200.patch	13,4 ko	27 juillet 2020	Nicolas Roche
0001-profile_views-add-a-profil-page-to-manage-authorized.patch	13,1 ko	27 juillet 2020	Nicolas Roche