Authentic 2 - Development #20696

Porter la gestion des clients OIDC dans le /manage

14 décembre 2017 12:36 - Mikaël Ates (de retour le 29 avril)

Statut:	Fermé	**Début:**	14 décembre 2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Aujourd'hui dans /admin.

Administration possible par le rôle Administrateur des Services.

Demandes liées:

Lié à Authentic 2 - Development #39406: Fournir dans le backoffice (/manage/)...	**Fermé**	**30 janvier 202005 octobre 2020**
Lié à Authentic 2 - Development #64649: Personnalisation de l'interface au SS...	**Fermé**	**28 avril 2022**

Révisions associées

Révision 39e2c463 - 08 juillet 2022 10:16 - Serghei Mihai

manager: add OpenID service handling (#20696)

Historique

#1 - 28 avril 2022 14:56 - Mikaël Ates (de retour le 29 avril)

- Lié à Development #39406: Fournir dans le backoffice (/manage/) des écrans de configuration de la gestion et de la fourniture des identités ajouté

#2 - 11 mai 2022 10:46 - Serghei Mihai

- Assigné à mis à Serghei Mihai

- Planning mis à Non

#5 - 11 mai 2022 12:12 - Serghei Mihai

Avant de coder il faudrait établir les champs exposés dans le formulaire d'ajout/édition, car tous les attributs visibles dans l'admin ne sont pas parlants/compréhensibles (même par les CPTs).
Et sur la base de ces champs faire une doc.

En plus des champs exposés déjà (nom, slug, collectivité, url de retour quand non-autorisé) je propose:

- URIs de redirection
- URIs de redirection après déconnexion
- URI de déconnexion frontchannel
- Politique des identifiants
- Algo de signature du token
- URL d'accueil
- Logo
- Couleur
- Mode d'autorisation
- Processus d'autorisation

Les claims ne seront pas exposés car on n'a presque jamais eu de demande de modification de ceux-ci.
Les client_id et client_secret seront affichés sur la page du service sans possibilité de les modifier.

#7 - 11 mai 2022 12:37 - Frédéric Péters

> Les claims ne seront pas exposés car on n'a presque jamais eu de demande de modification de ceux-ci.

Ça fait partie des demandes actuelles Strasbourg et sur les situations où il faut envoyer un gender qu'on base sur le title, ça veut dire qu'on devra quand même aller dans l'admin; ok pour que ça ne soit pas présent dans ce ticket mais avis perso ça devra venir à un moment.

#8 - 30 mai 2022 09:27 - Serghei Mihai

- Fichier 0001-manager-add-OpenID-service-handling-20696.patch ajouté

- Fichier 3.png ajouté

- Fichier 2.png ajouté

- Fichier 1.png ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Proposition d'ajouter les claims par défaut lors de la création d'un service OIDC, puis depuis la page du service pouvoir gérer les claims.
Il y a un peu de style à faire pour les boutons "Modifier" et "Supprimer" des claims, je fais un ticket gadjo.

#9 - 30 mai 2022 09:34 - Frédéric Péters

De la première capture je ne pense pas qu'on ait ailleurs de présentation en tableau, on privilégie soit libellé: valeur, soit libellé retour à la ligne valeur.

De la deuxième capture d'écran je dirais qu'il ne faut pas ouvrir en popup la création (ou la limiter aux champs strictement nécessaires).

#10 - 30 mai 2022 10:21 - Benjamin Dauvergne

Frédéric Péters a écrit :

> De la deuxième capture d'écran je dirais qu'il ne faut pas ouvrir en popup la création (ou la limiter aux champs strictement nécessaires).

Oui pas de popup, pour les objets complexe qu'on édite peu ce n'est vraiment pas pratique.

#11 - 30 mai 2022 16:12 - Serghei Mihai

- Fichier 0001-manager-add-OpenID-service-handling-20696.patch ajouté

- Fichier 1.1.png ajouté

Frédéric Péters a écrit :

> De la première capture je ne pense pas qu'on ait ailleurs de présentation en tableau, on privilégie soit libellé: valeur, soit libellé retour à la ligne valeur.

Ok, je suis parti sur "libellé : valeur" pour que les claims soient visibles à l'écran sans scroll.

> De la deuxième capture d'écran je dirais qu'il ne faut pas ouvrir en popup la création (ou la limiter aux champs strictement nécessaires).

Ok, pas de popup pour l'ajout du service.

#12 - 09 juin 2022 14:33 - Paul Marillonnet

Après un premier essai rapide en local :
· cela reste une popup lors de la modification du service (pas sûr que ce soit le comportement souhaité ?)

· une erreur de validation à la modification décale la popup seulement sur la partie droit de l'écran (cf capture).

· une première erreur de validation, ensuite corrigée, bloque définitivement la popup. Il n'y a plus moyen de valider le formulaire une fois l'erreur corrigée.

· on n'a perdu la fonctionnalité de complétion de la valeur des claims telle que proposée dans le /admin/, je pense que c'est utile de conserver ça.

· il n'y a nulle part où voir quels ont été les client_id et client_secret générés à la création du client. Je pense qu'il faut les faire apparaître en lecture seule.

· on s'attendrait à pouvoir éditer aussi la liste des "rôles visibles uniquement de ce service", mais ce n'est pas le cas. Est-ce qu'il y a une raison à laisser en édition la liste des "rôles autorisés à se connecter à ce service" mais pas celle des "rôles visibles uniquement de ce service" ?

Une première lecture en diagonale du code, je vois un

```
+    def get_object(self, queryset=None):
+        service = super().get_object(queryset)
+        if hasattr(service, 'oidcclient'):
+            self.model = OIDCClient
```

```
+             return service.oidcclient
+         return service
```

Je retrouve nulle part dans le code le moment où on rattache le client via un attribut oidcclient sur cette classe de base service (service.oidcclient). Je loupe un truc parce que ça marche en local, mais je ne vois pas quoi. De ma compréhension de l'affaire, la classe OIDCClient hérite de service et donc il faudrait manier le code de façon à tester quelque chose comme isinstance(service, OIDCClient) plutôt que @hasattr(service, 'oidcclient'), non ? Bref, je loupe un truc.

#13 - 09 juin 2022 14:34 - Paul Marillonnet

- Fichier validation_glitch.png ajouté

(Et la capture susmentionnée.)

#14 - 10 juin 2022 11:49 - Serghei Mihai

- Fichier 0001-manager-add-OpenID-service-handling-20696.patch ajouté

Paul Marillonnet a écrit :

> · cela reste une popup lors de la modification du service (pas sûr que ce soit le comportement souhaité ?)

De manière générale pour les services le bouton "Modifier" ouvre une popup. Je ne modifie pas ce comportement.

> · une erreur de validation à la modification décale la popup seulement sur la partie droit de l'écran (cf capture).

Ce n'est pas le cas chez moi. C'est pas lié à la conf de tes écrans?

> · une première erreur de validation, ensuite corrigée, bloque définitivement la popup. Il n'y a plus moyen de valider le formulaire une fois l'erreur corrigée.

C'est un autre pépin car existe déjà en prod, par ex: https://connexion-publik.entrouvert.com/manage/services/2/

> · on n'a perdu la fonctionnalité de complétion de la valeur des claims telle que proposée dans le /admin/, je pense que c'est utile de conserver ça.

J'ai jamais prêté attention qu'il y avait des suggestions de complétion. Rajouté.

> · il n'y a nulle part où voir quels ont été les client_id et client_secret générés à la création du client. Je pense qu'il faut les faire apparaître en lecture seule.

Oops, remis.

> · on s'attendrait à pouvoir éditer aussi la liste des "rôles visibles uniquement de ce service", mais ce n'est pas le cas. Est-ce qu'il y a une raison à laisser en édition la liste des "rôles autorisés à se connecter à ce service" mais pas celle des "rôles visibles uniquement de ce service" ?

Je n'ai pas touché à cette partie et il me semble qu'il n'est pas possible d'ajouter des rôles visibles uniquement de ce service. Ex: https://connexion-publik.entrouvert.com/manage/services/2/

> Une première lecture en diagonale du code, je vois un
> [...]
> Je retrouve nulle part dans le code le moment où on rattache le client via un attribut oidcclient sur cette classe de base service (service.oidcclient).

C'est lié à l'héritage par OIDCClient de Service. Il y a une rélation OneToOne qui s'établit entres la classe parente et fille, le parent ayant un accessor vers la classe fille qui raise une AttributeError si la classe fille n'existe pas.

> De ma compréhension de l'affaire, la classe OIDCClient hérite de service et donc il faudrait manier le code de façon à tester quelque chose comme isinstance(service, OIDCClient) plutôt que @hasattr(service, 'oidcclient'), non ?

Non, car dans cette vue on opére avec les instances de Service et isinstance(service, OIDCClient) sera toujours faux.
Je n'ai pas trouvé d'autre moyen de vérifier le type de la classe fille.

#15 - 13 juin 2022 15:01 - Paul Marillonnet

Ok, merci pour tes explications, il me manquait deux trois billes pour comprendre le truc.

Tout relu, le code est clair mais le seul truc qui me gêne un peu c'est le {{ service_block|safe }}. Ça m'a l'air trop peu django-esque de rendre un si gros bout de html directement dans la vue puis de le passer dans le gabarit final avec ce filtre safe ensuite.
Intuitivement, j'aurais bien vu un {% include extra_details %} avec cette valeur extra_details initialisée dans la vue à "authentic2/manager/oidc_service_detail.html", et en passant aussi le reste du contexte nécessaire au rendu de ce sous-gabarit (bien sûr pour le reste des services non OIDC ce extra_details n'est pas défini et donc cette balise include reste sans effet).

Autre chose encore et vraiment du détail, mais sur tous les titres "Add OpenID Claim", "Add OpenID service", etc. j'aurais bien vu un s/OpenID/OIDC/ pour éviter la confusion (OpenID est encore un autre protocole[1], ancêtre d'OIDC et pas du tout basé sur OAuth 2.0, et obsolète maintenant).

1. https://openid.net/specs/openid-authentication-2_0.html

#16 - 20 juin 2022 11:01 - Serghei Mihai

- Fichier 0001-manager-add-OpenID-service-handling-20696.patch ajouté

Paul Marillonnet a écrit :

> Tout relu, le code est clair mais le seul truc qui me gêne un peu c'est le {{ service_block|safe }}. Ça m'a l'air trop peu django-esque de rendre un si gros bout de html directement dans la vue puis de le passer dans le gabarit final avec ce filtre safe ensuite.

J'ai suivi le même principe que les blocs de login et inscription qui font leur rendu HTML et l'incluent dans un template global. Mais c'est plus propre, en effet, d'inclure un template dédié.

> Autre chose encore et vraiment du détail, mais sur tous les titres "Add OpenID Claim", "Add OpenID service", etc. j'aurais bien vu un s/OpenID/OIDC/ pour éviter la confusion (OpenID est encore un autre protocole[1], ancêtre d'OIDC et pas du tout basé sur OAuth 2.0, et obsolète maintenant).

Ok, done (jenkins devrait être contenu sous peu).

#17 - 21 juin 2022 11:35 - Paul Marillonnet

Serghei Mihai a écrit :

> J'ai suivi le même principe que les blocs de login et inscription qui font leur rendu HTML et l'incluent dans un template global. Mais c'est plus propre, en effet, d'inclure un template dédié.

Top.

> Ok, done (jenkins devrait être contenu sous peu).

Merci.

J'ai testé et tout me va, il me reste une dernière interrogation (que je n'avais pas relevée à ma dernière relecture, mes excuses), pourquoi ne pas utiliser le widget de choix de couleur natif du navigateur pour la couleur du client ? Ça a l'air supporté partout de façon systématique (sauf IE mais tant pis, un admin a2 sous IE ne pourra pas choisir la couleur du client OIDC, pas bien dramatique, non ?)

#18 - 21 juin 2022 12:29 - Valentin Deniaud

Il y aurait moyen de mettre les vues/templates/urls/form dans le module authentic2_idp_oidc ? Dans l'idée de ne pas charger le code générique, puisqu'il faudra ajouter SAML et CAS par la suite. Ça vaudrait aussi pour get_oidc_service_data qui pourrait être une méthode du modèle OIDCClient.

Pour rapprocher un peu le code de ce qui a été fait pour les moyens d'authentification je verrais bien OIDCClient qui définisse un manager_form_class, ce qui permettrait de s'économiser la gymnastique fields.extend(oidc_app_settings.MANAGER_FIELDS).

#19 - 21 juin 2022 12:47 - Paul Marillonnet

Valentin Deniaud a écrit :

> Il y aurait moyen de mettre les vues/templates/urls/form dans le module authentic2_idp_oidc ? Dans l'idée de ne pas charger le code générique, puisqu'il faudra ajouter SAML et CAS par la suite.

CAS on pourra s'épargner cela (#34257, pas un seul raccordement encore actif chez nous à ma connaissance), et je ne sais pas dans quelle mesure on a intérêt à ajouter SAML au lieu de dire "OIDC everywhere" pour ce qui est des raccordements avec a2 en tant qu'IdP (?)

#20 - 29 juin 2022 10:10 - Serghei Mihai

- Fichier 0001-manager-add-OpenID-service-handling-20696.patch ajouté

Vos remarques prises en compte.

#21 - 29 juin 2022 10:30 - Valentin Deniaud

- self.model = OIDCClient et model = None, j'ai pas l'impression qu'il y ait d'usage de ça ?
- Est-ce qu'il y a une vraie utilité au setting MANAGER_FIELDS ? Je ne suis même pas sûr que le changer fonctionne sans redémarrage de l'application. À la place on pourrait avoir de manière plus classique la définition des champs dans le formulaire et ensuite accéder à form._meta.fields.

À part ça c'est OK pour moi (mais je laisse Paul valider, je n'ai pas testé pour de vrai).

#22 - 29 juin 2022 12:36 - Serghei Mihai

- Fichier 0001-manager-add-OpenID-service-handling-20696.patch ajouté

Valentin Deniaud a écrit :

> - self.model = OIDCClient et model = None, j'ai pas l'impression qu'il y ait d'usage de ça ?

Bien vu, j'ai retiré.

> - Est-ce qu'il y a une vraie utilité au setting MANAGER_FIELDS ? Je ne suis même pas sûr que le changer fonctionne sans redémarrage de l'application. À la place on pourrait avoir de manière plus classique la définition des champs dans le formulaire et ensuite accéder à form._meta.fields.

C'est pour laisser la main de changer cette liste dans le settings d'un tenant, si besoin.
C'est censé de fonctionner sans redémarrage.

#23 - 29 juin 2022 12:48 - Valentin Deniaud

Serghei Mihai a écrit :

> C'est pour laisser la main de changer cette liste dans le settings d'un tenant, si besoin.
> C'est censé de fonctionner sans redémarrage.

Du coup j'ai testé et ça ne fonctionne que pour les display_fields, les champs du formulaire restent les mêmes, la classe étant chargée une seule fois au démarrage de l'appli. Je propose de se passer de cette feature :)

#24 - 30 juin 2022 12:16 - Serghei Mihai

- Fichier 0001-manager-add-OpenID-service-handling-20696.patch ajouté

D'accord.

#25 - 04 juillet 2022 11:50 - Serghei Mihai

- Lié à Development #64649: Personnalisation de l'interface au SSO : ne pas mettre de lien par défaut sur le nom et le logo du service si l'url n'est pas définie ajouté

#26 - 08 juillet 2022 10:11 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Serghei Mihai a écrit :

> D'accord.

Et de mon côté toutes mes remarques ont été prises en compte. Je viens de tester en local, juste un tout petit rebase manuel à faire dans les scss du backoffice car #65482 est passé entre temps, sinon c'est nickel !

#27 - 08 juillet 2022 10:32 - Serghei Mihai

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

```
commit 9788c39e93805ef0c472c9136f21da41fe177ccd (origin/main)
Author: Serghei Mihai <smihai@entrouvert.com>
Date:   Fri Jul 8 10:31:47 2022 +0200
```

```
    translations update

commit 39e2c46326f86d274be4b7fe063e7a6c634e21a2
Author: Serghei Mihai <smihai@entrouvert.com>
Date:   Thu May 12 17:27:06 2022 +0200

    manager: add OpenID service handling (#20696)
```

#28 - 08 juillet 2022 11:14 - Transition automatique

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

#29 - 11 septembre 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-manager-add-OpenID-service-handling-20696.patch	18,3 ko	30 mai 2022	Serghei Mihai
3.png	132 ko	30 mai 2022	Serghei Mihai
2.png	129 ko	30 mai 2022	Serghei Mihai
1.png	113 ko	30 mai 2022	Serghei Mihai
0001-manager-add-OpenID-service-handling-20696.patch	18,4 ko	30 mai 2022	Serghei Mihai
1.1.png	120 ko	30 mai 2022	Serghei Mihai
validation_glitch.png	247 ko	09 juin 2022	Paul Marillonnet
0001-manager-add-OpenID-service-handling-20696.patch	19,6 ko	10 juin 2022	Serghei Mihai
0001-manager-add-OpenID-service-handling-20696.patch	19,7 ko	20 juin 2022	Serghei Mihai
0001-manager-add-OpenID-service-handling-20696.patch	27,2 ko	29 juin 2022	Serghei Mihai
0001-manager-add-OpenID-service-handling-20696.patch	26,5 ko	29 juin 2022	Serghei Mihai
0001-manager-add-OpenID-service-handling-20696.patch	25,7 ko	30 juin 2022	Serghei Mihai