Authentic 2 - Development #39406

Fournir dans le backoffice (/manage/) des écrans de configuration de la gestion et de la fourniture des identités

30 janvier 2020 10:26 - Paul Marillonnet

Statut:	Fermé	**Début:**	30 janvier 2020
Priorité:	Normal	**Echéance:**	05 octobre 2020
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

En l'état actuel il faut passer par le /admin/ django, dont l'interface utilisateur actuelle ne correspond pas aux choix de simplification et de masquage de la complexité des écrans de configuration dans Publik.

De là à, comme discuté par courriel, voir disparaître le /admin/, je ne sais pas.
Mais, encore pour rebondir sur ces discussions, ça pourrait notamment réduire la charge de travail nécessaire de consolidation de la documentation d'Authentic.

Demandes liées:

Lié à Authentic 2 - Development #5541: Add a page to manage providers	**Fermé**	**19 septembre 2014**
Lié à Authentic 2 - Development #6648: Allow managing LDAP servers from the m...	**Nouveau**	**09 mars 2015**
Lié à Plugin FS FranceConnect - Development #29246: Interface de configuration	**Fermé**	**20 décembre 2018**
Lié à Authentic 2 - Development #41671: écran de configuration de la connexio...	**Fermé**	**14 avril 2020**
Lié à Authentic 2 - Development #41876: pouvoir agir sur l'ordre d'affichage ...	**Fermé**	**20 avril 2020**
Lié à Gadjo - Development #47132: avoir une icône pour la gestion de l'authen...	**Rejeté**	**29 septembre 2020**
Lié à Gadjo - Development #47902: style pour les titre des sections désactivées	**Fermé**	**20 octobre 2020**
Lié à Gadjo - Development #47901: style pour lien-bouton en titre de section	**Fermé**	**20 octobre 2020**
Lié à Gadjo - Development #48140: ne pas afficher (optionnel) sur les cases à...	**Fermé**	**30 octobre 2020**
Lié à Publik - Development #49198: Paramétrage poussé d'Authentic via l'inter...	**Fermé**	**08 décembre 2020**
Lié à Authentic 2 - Development #53902: avoir une classe de base pour les mod...	**Fermé**	**10 mai 2021**
Lié à Authentic 2 - Development #20697: Avoir une interface de configuration ...	**Fermé**	**14 décembre 2017**
Lié à Authentic 2 - Development #20696: Porter la gestion des clients OIDC da...	**Fermé**	**14 décembre 2017**

Historique

#1 - 30 janvier 2020 10:32 - Benjamin Dauvergne

Ça fait un gros ticket quand même.

#2 - 30 janvier 2020 10:33 - Paul Marillonnet

Je voyais vraiment ça comme un « ticket-chapeau ».

#3 - 30 janvier 2020 10:40 - Mikaël Ates (de retour le 29 avril)

Qui chapeauterait des tickets comme #5541 et #6648 ?

#4 - 30 janvier 2020 11:01 - Paul Marillonnet

- Lié à Development #5541: Add a page to manage providers ajouté

#5 - 30 janvier 2020 11:01 - Paul Marillonnet

- Lié à Development #6648: Allow managing LDAP servers from the manager ajouté

#6 - 30 janvier 2020 11:03 - Paul Marillonnet

Mikaël Ates a écrit :

> Qui chapeauterait des tickets comme #5541 et #6648 ?

Merci (je n'avais pas pensé à chercher en anglais des sous-tickets candidats préexistants).

#7 - 14 avril 2020 13:13 - Frédéric Péters

- Lié à Development #29246: Interface de configuration ajouté

#8 - 14 avril 2020 13:13 - Frédéric Péters

- Lié à Development #41671: écran de configuration de la connexion par mot de passe ajouté

#9 - 18 avril 2020 13:50 - Frédéric Péters

- Fichier login-settings.png ajouté

À titre d'illustration/maquette possible, sur la forme que ça pourrait prendre, pour qui voudrait avancer là-dessus, image attachée.

#10 - 18 avril 2020 15:59 - Paul Marillonnet

C'est de la balle, merci pour la maquette. Dès que j'ai bouclé la migration à django 2.2 je m'y colle.

#11 - 20 avril 2020 11:38 - Serghei Mihai

- Lié à Development #41876: pouvoir agir sur l'ordre d'affichage des blocs d'authentification sur la page de connexion ajouté

#12 - 20 avril 2020 12:07 - Frédéric Péters

- Fichier a2-add-provider.png ajouté

- Fichier a2-reorder.png ajouté

Maquette avec la fenêtre d'ajout d'un fournisseur (exemple, on peut aussi imaginer quelques champs supplémentaires/communs, genre un libellé); et maquette avec l'ordre d'affichage.

#13 - 20 avril 2020 14:05 - Benjamin Dauvergne

Il faut prendre en compte les OUs, en fait ces écrans devraient venir en dessous de chaque OU, ça ne peut pas être global.

#14 - 20 avril 2020 14:10 - Frédéric Péters

Les méthodes d'authentification viennent avant l'authentification de l'utilisateur, ces paramètres ne sont aujourd'hui pas liés à une OU, comment cela se lierait-il à une OU ?

#15 - 20 avril 2020 15:14 - Benjamin Dauvergne

À part login/mdp sur modèles toutes les autres sont liées à une OU (ldap, oidc) sauf SALM où je pense que ça fait juste n'importe quoi actuellement (des utilisateurs sans OU).

#16 - 20 avril 2020 15:32 - Frédéric Péters

Ok, mais ça indique pour moi plutôt alors qu'il faut inclure un sélecteur d'OU dans le paramétrage, parce qu'on reste sur une seule page de connexion.

Pour la partie LDAP, je ne l'imaginais pas sur cet écran. (un écran similaire, avec sans doute là aussi un a priori pour une sélection de l'OU dans le paramétrage, plutôt qu'un écran par OU).

#17 - 20 avril 2020 15:41 - Benjamin Dauvergne

Frédéric Péters a écrit :

> Ok, mais ça indique pour moi plutôt alors qu'il faut inclure un sélecteur d'OU dans le paramétrage, parce qu'on reste sur une seule page de connexion.
>
> Pour la partie LDAP, je ne l'imaginais pas sur cet écran. (un écran similaire, avec sans doute là aussi un a priori pour une sélection de l'OU dans le paramétrage, plutôt qu'un écran par OU).

Ça veut dire que plusieurs collectivités ne pourront jamais gérer leur raccordement LDAP/SAML elle même sans un cas multico, sauf à toucher à tout; j'ai toujours envisagé les OU comme le moyen de cloisonner le BO d'a2 en mode multitenant dans une même instance (et ça marche déjà pour rôles et les utilisateurs). Je trouverai dommage d'abandonner cette objectif pour les services.

Ça n'empêche pas que certains trucs resteront globaux comme :

- la protection contre les attaque force brut login/mdp (parce qu'on a qu'un formulaire pour tout le monde)
- les certificats RSA/DSA pour SAML ou OIDC (parce qu'on qu'un idp pour tout le monde)

La gestion des mots de passe, de la validation des mails, de l'unicité du mail ou du username, et la politique de nettoyage des comptes sont déjà par OU.

#18 - 20 avril 2020 16:30 - Frédéric Péters

> veut dire que plusieurs collectivités ne pourront jamais gérer leur raccordement LDAP/SAML elle même dans un cas multico

Le même écran peut être utilisé, en affichant uniquement les raccordements liés à l'OU en question.

Je trouve utile pour l'administrateur d'avoir cette vue d'ensemble, plutôt qu'avoir à visiter n OU en se disant que peut-être la commune unetelle est reliée à un LDAP. (et je pense aussi ce cas de l'administrateur technique "global" plus commun que la délégation du paramétrage des annuaires à chacune des communes d'une interco).

#19 - 20 avril 2020 17:31 - Benjamin Dauvergne

Là ok.

#20 - 01 mai 2020 10:22 - Paul Marillonnet

- Assigné à mis à Paul Marillonnet

#21 - 13 juillet 2020 10:52 - Serghei Mihai

- Assigné à Paul Marillonnet supprimé

Je vais prendre à mon retour de congés (le 10 août).

#22 - 10 août 2020 17:41 - Serghei Mihai

- Echéance mis à 14 septembre 2020

- Assigné à mis à Serghei Mihai

#23 - 14 septembre 2020 13:52 - Serghei Mihai

- Echéance changé de 14 septembre 2020 à 28 septembre 2020

#24 - 24 septembre 2020 09:16 - Serghei Mihai

- Echéance changé de 28 septembre 2020 à 05 octobre 2020

Ça sera pour la prochaine itération.

#27 - 29 septembre 2020 16:13 - Serghei Mihai

- Lié à Development #47132: avoir une icône pour la gestion de l'authentification ajouté

#28 - 26 octobre 2020 10:11 - Serghei Mihai

- Lié à Development #47902: style pour les titre des sections désactivées ajouté

#29 - 26 octobre 2020 10:11 - Serghei Mihai

- Lié à Development #47901: style pour lien-bouton en titre de section ajouté

#30 - 29 octobre 2020 15:24 - Serghei Mihai

- Statut changé de Nouveau à En cours

Branche à jour avec des tests.
Il manque la possibilité d'ordonner les blocs d'authentification.

J'ai perdu pas mal de temps à essayer de faire un widget permettant de définir le mapping entre les attributs SAML/OIDC et ceux du profil usager, sans arriver à un résultat qui me plaise. Je me laisse ça comme amélioration pour plus tard et me contente d'un champ JSON.

Une petite vidéo de l'usage (les traductions ne sont pas faites): https://perso.entrouvert.org/~smihai/authenticators.mp4

#31 - 29 octobre 2020 18:34 - Frédéric Péters

J'ai juste regardé la vidéo.

Je trouve que le feedback du titre grisé est suffisant, plutôt qu'aller décaler en hauteur les blocs via un (django.contrib.)message.

Utile aussi de travailler les styles pour réduire la hauteur, cf par exemple hobo qui range les scopes oidc en colonnes.

Communément il me semble qu'on ajoute plutôt du SAML en 1/ pointant une URL 2/ uploadant un fichier; je trouve curieuse l'utilisation d'un textarea.
Pour l'oidc je me demande à quel point le .well-known/... est courant dans les implémentations, s'il est courant il pourrait y avoir un seul champ URL, plutôt qu'un champ par endpoint.

De manière plus générale, si une popup est plus haute que l'écran autant en faire une vraie page; mais plutôt je serais pour que l'ajout se fasse en réduisant le nombre de champs, libre ensuite d'ajuster le paramétrage. (par exemple pas besoin de lister les scopes si la valeur par défaut est ok).

~~

Je pensais aussi que côté gadjo on n'affichait plus "(optionnel)" pour les cases à cocher; et les formulaires d'ajout et de modification devraient être cohérents, là on a des astérisques à l'ajout et des (optionnel) à la modification.

#32 - 30 octobre 2020 10:48 - Serghei Mihai

- Fichier authentic-sp-saml.png ajouté

- Fichier Authenticators-FC.png ajouté

Frédéric Péters a écrit :

> Je trouve que le feedback du titre grisé est suffisant, plutôt qu'aller décaler en hauteur les blocs via un (django.contrib.)message.

Je trouvais utile d'afficher le message notamment quand on désactive un bloc qui n'est visible qu'en scrollant la page, mais le grisé devrait suffire.

> Utile aussi de travailler les styles pour réduire la hauteur, cf par exemple hobo qui range les scopes oidc en colonnes.

En effet, zappé les styles, rajouté.

> Communément il me semble qu'on ajoute plutôt du SAML en 1/ pointant une URL 2/ uploadant un fichier; je trouve curieuse l'utilisation d'un textarea.

J'ai fait un peu par analogie avec la gestion des SP dans l'admin, ou on pointe une URL ou un fichier mais c'est le contenu qui est important pour prendre en compte le SP.
Cela permet aussi un peu de "voir" les métadonnées. Parmi tes suggestions je préfère l'upload d'un fichier au lieu de pointer une URL car dans pas mal de cas quand nous demandons les métadonnées on nous file un fichier et non une URL.

> Pour l'oidc je me demande à quel point le .well-known/... est courant dans les implémentations, s'il est courant il pourrait y avoir un seul champ URL, plutôt qu'un champ par endpoint.

J'en ai aucune idée. Peut-être les GI men en savent plus. Ici je suis parti sur un ModelForm.

> De manière plus générale, si une popup est plus haute que l'écran autant en faire une vraie page; mais plutôt je serais pour que l'ajout se fasse en réduisant le nombre de champs, libre ensuite d'ajuster le paramétrage. (par exemple pas besoin de lister les scopes si la valeur par défaut est ok).

Sur un écran dont la hauteur fait 800px la popup FC s'affiche entièrement.
Idée à côté: il y aurait peut-être ici un peu de travail sur l'amélioration des libellés des scopes, reprendre ceux qui sont définis dans le backoffice client dans FC.

> ~~
>
> Je pensais aussi que côté gadjo on n'affichait plus "(optionnel)" pour les cases à cocher;

Cela a été fait uniquement dans publik-base-theme: #46436, je fais un ticket pour gadjo.

> et les formulaires d'ajout et de modification devraient être cohérents, là on a des astérisques à l'ajout et des (optionnel) à la modification.

en effet, zappé l'attribut css_class des formulaires.

#33 - 30 octobre 2020 10:50 - Serghei Mihai

- Lié à Development #48140: ne pas afficher (optionnel) sur les cases à cocher ajouté

#34 - 30 octobre 2020 12:00 - Frédéric Péters

> > De manière plus générale, si une popup est plus haute que l'écran autant en faire une vraie page (...)
>
> Sur un écran dont la hauteur fait 800px la popup FC s'affiche entièrement.

Je parlais de manière générale (en voyant dans ta vidéo que l'ajout SAML dépasse), surtout pour noter que réduire le nombre de champs initialement dans la popup serait je trouve une bonne idée.

#35 - 03 novembre 2020 12:28 - Serghei Mihai

- Fichier Authenticators - OIDC.png ajouté

- Fichier Authenticators - SAML.png ajouté

Ok, je fais 2 formulaires séparés pour l'ajout et l'édition d'un authenticator.
Rajouté également la possibilité de changer l'ordre d'affichage.

#36 - 03 novembre 2020 23:57 - Benjamin Dauvergne

Il est parti beaucoup trop gros ce ticket, j'aurai préféré avoir une vision de ce qui allait être fait techniquement en dehors des mockups.

Le fait de vouloir mettre plusieurs formulaires sur une seule page rend les choses très complexes (typiquement pour les mappings ça va être galère, autant gérer ça sur plusieurs pages), je préférerai une page de visualisation, avec des informations minimales (le nom, le type, si c'est conditionné ou pas) et qui permet de gérer l'ordre et changer des petits choses via des popups comme le nom d'un bouton, un message d'intro, la condition, etc... Après pour chaque type de système d'authentification une page formulaire de création et édition, ou alors une page de visualisation plus complète avec pour chaque élément un mini-formulaire en popup (pour la condition d'affichage, à la façon des formulaires/workflow w.c.s.).

Chaque système d'authentification devrait tenir sur 2/3 lignes pas plus sur cette page d'accueil.

Aussi un stockage des settings je ne pense pas que ça faisait parti des choses dont on avait parlé les dernières fois; ça va marcher pour FranceConnect parce qu'on a jamais qu'une seule instance et puis devenir compliqué pour le reste. Je pense plutôt à quelque chose de plus simple comme un modèle de ce genre :

Ça me dérange pas qu'on introduise un stockage de settings, mais j'ai peu que si on commence à s'en servir pour un truc un peu structuré on ne s'en passe jamais et on se sente permis d'y mettre n'importe quoi.

```
Authenticator :
 - id
 - uuid
 - name
 - order
 - slug : slugfield
 - type : charfield = (login/password, fc)
 - data : jsonfield = (ex. pour FC) {'platform'': 'integration', 'client_id': 'xxx', 'mappings': [...]}
                      (ex. pour login/password) {'use_ou_field': False, 'accept_email_authentication': .., 're
try_timeout_factor': .. ,'retry_timeout_duration':...} (<- on est pas obligé de tout transférer des settings e
t exposer d'un coup c'est pour donner une idée)
```

Ça n'est pas plus compliqué qu'un stockage de setting mais c'est plus propre et ça permet de se débarrasser des settings.

J'ai commencé ça mettre les choses dans authentic2/apps, continuons.

Après pour la définition des pages/formulaires on repart de classes AuthenticatorType qui fournissent des URLs et des formulaires pour éditer data (à la manière des modèles passerelle).

Coté OIDC et SAML on pourra définir un modèle hérité et ne pas tout mettre dans data si ça un sens (et pour OIDC faire hériter OIDCProvider de Authenticator) pour essayer de faire converger les choses.

#38 - 04 novembre 2020 14:34 - Serghei Mihai

- Fichier Authenticators-Home.png ajouté

Benjamin Dauvergne a écrit :

> Il est parti beaucoup trop gros ce ticket, j'aurai préféré avoir une vision de ce qui allait être fait techniquement en dehors des mockups.
>
> Le fait de vouloir mettre plusieurs formulaires sur une seule page rend les choses très complexes (typiquement pour les mappings ça va être galère, autant gérer ça sur plusieurs pages), je préférerai une page de visualisation, avec des informations minimales (le nom, le type, si c'est conditionné ou pas) et qui permet de gérer l'ordre et changer des petits choses via des popups comme le nom d'un bouton, un message d'intro, la condition, etc... Après pour chaque type de système d'authentification une page formulaire de création et édition, ou alors une page de visualisation plus complète avec pour chaque élément un mini-formulaire en popup (pour la condition d'affichage, à la façon des formulaires/workflow w.c.s.).

> Chaque système d'authentification devrait tenir sur 2/3 lignes pas plus sur cette page d'accueil.

Ok, ça serait quelque chose comme dans la capture jointe.

> Ça me dérange pas qu'on introduise un stockage de settings, mais j'ai peu que si on commence à s'en servir pour un truc un peu structuré on ne s'en passe jamais et on se sente permis d'y mettre n'importe quoi.

Le but de ce stockage est de ne pas chambouler tout le fonctionnement existant qui se base sur des settings.json tapés dans les répértoires des tenants ou des variables transmises par Hobo.
Certains settings (surtout pour LoginPassword) avec des valeurs par défaut ne sont pas exposés dans le manager mais ont un impact.

> J'ai commencé ça mettre les choses dans authentic2/apps, continuons.
>
> Après pour la définition des pages/formulaires on repart de classes AuthenticatorType qui fournissent des URLs et des formulaires pour éditer data (à la manière des modèles passerelle).
>
> Coté OIDC et SAML on pourra définir un modèle hérité et ne pas tout mettre dans data si ça un sens (et pour OIDC faire hériter OIDCProvider de Authenticator) pour essayer de faire converger les choses.

Je regarde tout ça.

#39 - 08 décembre 2020 05:52 - Pierre Cros

- Lié à Development #49198: Paramétrage poussé d'Authentic via l'interface graphique ajouté

#40 - 10 mai 2021 16:29 - Serghei Mihai

- Lié à Development #53902: avoir une classe de base pour les modèles de gestion des moyens d'authentification ajouté

#41 - 11 mai 2021 12:05 - Frédéric Péters

- Lié à Development #20697: Avoir une interface de configuration en backoffice permettant de poser des configurations aujourd'hui en settings ajouté

#42 - 28 avril 2022 14:56 - Mikaël Ates (de retour le 29 avril)

- Lié à Development #20696: Porter la gestion des clients OIDC dans le /manage ajouté

#43 - 19 septembre 2022 17:19 - Valentin Deniaud

- Statut changé de En cours à Fermé

Travail complété dans les tickets liés.

Fichiers

login-settings.png	162 ko	18 avril 2020	Frédéric Péters
a2-reorder.png	106 ko	20 avril 2020	Frédéric Péters
a2-add-provider.png	105 ko	20 avril 2020	Frédéric Péters
authentic-sp-saml.png	175 ko	30 octobre 2020	Serghei Mihai
Authenticators-FC.png	152 ko	30 octobre 2020	Serghei Mihai
Authenticators - SAML.png	242 ko	03 novembre 2020	Serghei Mihai
Authenticators - OIDC.png	271 ko	03 novembre 2020	Serghei Mihai
Authenticators-Home.png	8,67 ko	04 novembre 2020	Serghei Mihai