Configuration lien d'identification unique (SSO)

DIMELO
29, rue du Louvre 75002 PARIS
Tél.: + 33(0)1 48 56 88 25
Fax. : + 33(0)1 74 18 00 14

1. Objet

Le présent document a pour objectif de présenter et de décrire la configuration de la fonctionnalité Single Sign-On (SSO).

Ce SSO doit être activé par nos soins avant sa mise en place.

Dans ce document, nous appelons « Serveur d'authentification » la plateforme centralisée permettant la gestion des utilisateurs de vos différentes applications. Son URL est sous la forme suivante : https://votre_nom.users.feedback20.com.

2. Description de la fonctionnalité

La fonctionnalité SSO se présente sous la forme d'une simple URL à générer et à placer sous forme de lien sur une page web, un mail, ...

Ce lien permet de créer dynamiquement des utilisateurs et/ou de les reloguer à leur compte sur une plateforme feedback2.0.

Cette URL de base (SSO simple) a la forme suivante:

https://URL_**DU_SERVEUR_D_AUTHENTIFICATION/cas/login?auth=sso&type=acceptor&service=URL_DE_VOTRE_APPLICATION&uuid=IDENTIFIANT &token=TOKEN&expires=DATE_EXPIRATION...**

Le principe fonctionnel est simple, quand un utilisateur utilise ce lien, il arrive sur le serveur d'authentification de votre plateforme feedback2.0 Les paramètres de l'url sont alors vérifiés ainsi que leur conformité (voir la section token).

Si les paramètres sont correctes alors :

- Si il n'existe pas de compte avec l'uuid fournis, le compte est créé avec les paramètres fournis (nom, prénom, email, ...) et l'utilisateur est connecté sous ce compte et redirigé vers l'application donné en paramètre service.
- Si le compte existait l'utilisateur est connecté sur le compte correspondant à l'uuid, et les attributs de l'utilisateur sont mis à jour avec ceux fournis dans l'url.

3. Liste des paramètres d'un lien SSO

Paramètre	Pris en compte dans le calcul du token ?	Requis	Exemple de valeur	Format
auth	NON	OUI	sso	«sso»
type	NON	OUI	acceptor	«acceptor»
service	NON	OUI	http://mondomain.ideas.feedback20.com	Une url valide
firstname	OUI	OUI	Renaud	Caractère alphabétique, apostrophe, tiret, chiffres
uuid	OUI	OUI	identifiant_unique_12	Tous caractères pouvant passer par un lien
expires	OUI	OUI	1249081200	Timestamp UNIX (= heure POSIX)
token	NON	OUI	bfc9396b7c710746b19a1297e70d1716	chaine hexadecimale
avatar_url	OUI	NON	http://google.com/logo.png	Une url valide d'image
email	OUI	NON	renaud.morvan@feedback20.com	Une adresse email valide
lastname	OUI	NON	Morvan	Caractère alphabétique, apostrophe, tiret, chiffres
charset	NON	NON	latin1	« latin1» ou «latin15» ou «winlatin1»

Paramètre	Pris en compte dans le calcul du token ?	Requis	Exemple de valeur	Format
role	OUI	NON	expert	Caractère alphabétique, chiffres, tiret bas

4. Détails des paramètres d'un lien SSO

L'URL accepte une série de paramètres. Les paramètres suivants sont obligatoires :

- **auth** : doit obligatoirement être **sso**.
- **type** : doit obligatoirement être **acceptor.**
- **service** : URL de l'application vers laquelle l'utilisateur va être redirigé.
- **firstname** : Prénom de l'utilisateur.
- **uuid** : Identifiant unique de l'utilisateur (exemple : email ou id dans votre base, ou son login sur votre application).
- **expires** : **Heure** sous le format « timestamp unix » (http://fr.wikipedia.org/wiki/Heure_UNIX) **à laquelle le lien SSO sera expiré**.

Un timestamp Unix est le nombre de seconde depuis le 1 janvier 1970 jusqu'à la heure dite. Exemple: 1er aout 2009 à 00:00 => 1249077600, si vous voulez faire expirer une heure plus tard alors expires= 1249077600 + 3600 = 1249081200. (L'avantage de ce format est qu'il est indépendant du fuseau horaire et tous les langages informatiques disposent des fonctions pour vous fournir cette représentation).

- **token** : Chaine de caractère calculée de façon déterministe pour la validation des paramètres spécifiés (voir par la suite : Calcul du token). Ce paramètre assure la sécurité des paramètres que vous avez choisis.
- **role** : Chaine de caractère représentant le rôle de l'utilisateur sur l'application. S'il est omis, il aura la valeur « user ».

5. Paramètres optionnels

Les paramètres suivants sont optionnels :

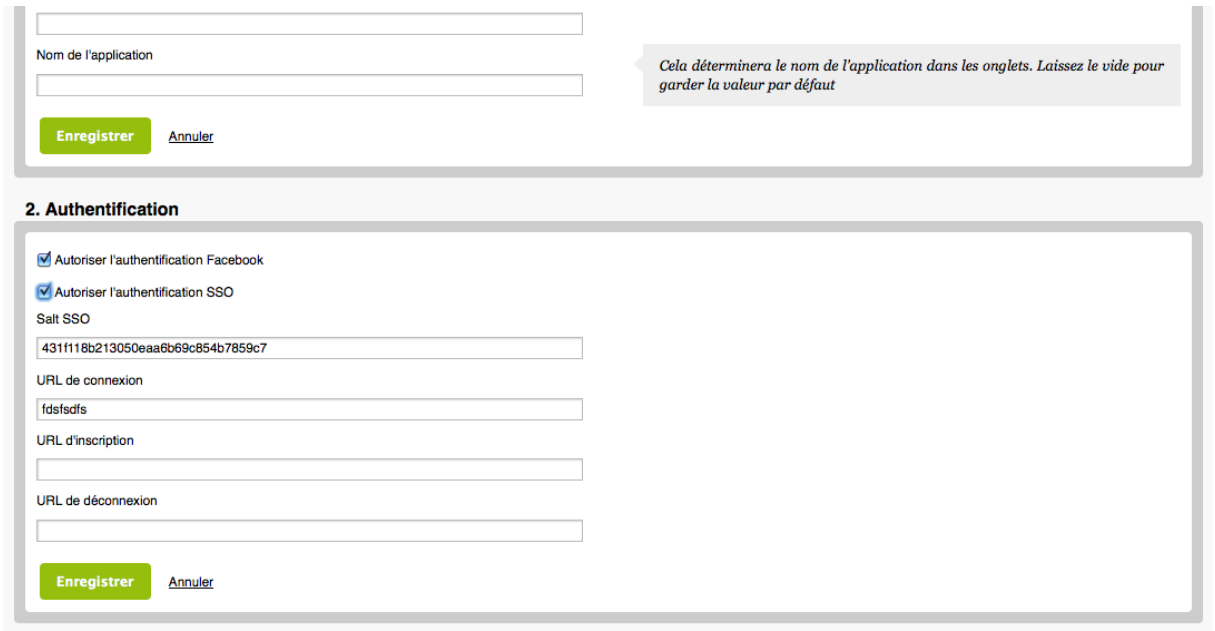
- **avatar_url** : URL de l'avatar de l'utilisateur (doit être une image).
- **email** : E-mail de l'utilisateur, si vous ne fournissez pas d'e-mail, l'utilisateur ne recevra pas d'e-mail de la part de l'application Feedback2.0 lors de nouveau commentaire par exemple.
- **lastname** : Nom de l'utilisateur.
- **charset** : Encodage des paramètres (Voir par la suite : Encodage des caractères).

6. Obtention du « salt »

Le **salt** est nécessaire dans le calcul du token. Ce salt est propre à chacune de vos applications. Si vous souhaitez créer un lien SSO pour votre application ideas vous **devez utiliser le salt correspondant**. Vous devez vous rendre dans l'interface d'administration du serveur d'authentification pour l'obtenir.

Allez dans l'onglet **Applications**, puis cliquez sur le lien **modifier** de l'application où vous souhaitez obtenir le salt ainsi qu'activer le SSO.

Vous devriez avoir l'écran suivant :



7. Calcul du token

Considérons l'utilisateur avec les paramètres suivants :

auth: sso
type: acceptor
firstname : Jean
email : jm@mail.com
uuid: jmar0112
avatar_url: http://avatar.com/jp.png
expires: 1249128000 (1 er aout 09 à midi heure de Paris)

Seuls les paramètres suivants sont pris en compte dans le calcul du token : **avatar_url**, **email**, **expires**, **firstname**, **lastname**, et **uuid** (Voir tableau).

Tous les autres paramètres (**auth**, **type**, **service**, …) ne seront **pas pris en compte** dans le calcul du token (ni donc dans la concaténation) mais restent obligatoire dans l'url.

Le rôle du token est de «signer» les paramètres que vous avez fournis, afin que personne ne puisse les modifier et prendre le contrôle d'un autre compte. Afin de signer les paramètres il faut les concaténer suivant une certaine formule et ensuite utiliser la fonction de hashage SHA1.

Par ordre alphabétique des noms de paramètres l'ordre est : avatar_url , email, expires, firstname, uuid. Le calcul du token se fait par concaténation des paramètres présent dans l'url suivant leur ordre alphabétique.

La concaténation des paramètres est de la forme:

'<nom du paramètre 1>-<valeur 1>:<nom du paramètre 2>-<valeur 2>:.....:<nom du paramètre n>-<valeur n> '

La concaténation des paramètres de notre exemple donne donc:

params = 'avatar_url-http://avatar.com/jp.png:email-jp@mail.com:expires-1249128000:firstname-Jean:uuid-jpmar0112'

Les paramètres ne doivent pas encore être passés par une "url encode" au moment de la génération du token. Pour le cas où les champs sont vides. Soit ils sont passés vide dans l'url et dans le calcul du token. Soit ils ne sont présents ni dans l'un, ni dans l'autre.

On concatène le salt aux paramètres précédant suivant la formule:

final = params + 'salt'

Le token est le résultat de la fonction SHA1 sur la chaîne finale :

token = sha1(final)

Le token aura donc pour valeur c5b3570f1a2973af44e78bfcb817131535a676a1 pour un salt ayant pour valeur bfc9396b7c710746b19a1297e70d1716

Donc le token sera c5b3570f1a2973af44e78bfcb817131535a676a1, c'est à dire sha1('avatar_url-http://avatar.com/jp.png:email-jp@mail.com:expires-1249128000:firstname-Jean:uuid-jpmar0112bfc9396b7c710746b19a1297e70d1716')

Le lien sso correspondants aux paramètres de l'exemple sera donc:

https://domain-test.users.feedback20.com/cas/login?auth=sso&type=acceptor&service=http://domain-test.ideas.feedback20.com&firstname=Jean&email=jm@mail.com&uuid=jmar0112&avatar_url=http://avatar.com/jp.png&expires=1249128000

8. Encodage des caractères

L'encodage des caractères peut être différent entre la plateforme intégrant le SSO et la plateforme feedback2.0. Si tel est le cas, il est nécessaire d'ajouter un paramètre supplémentaire.

La plateforme feedback2.0 utilise le l'encodage de caractères « unicode UTF-8 ».
Si votre plateforme utilise le même encodage il n'y a donc rien à paramètrer.

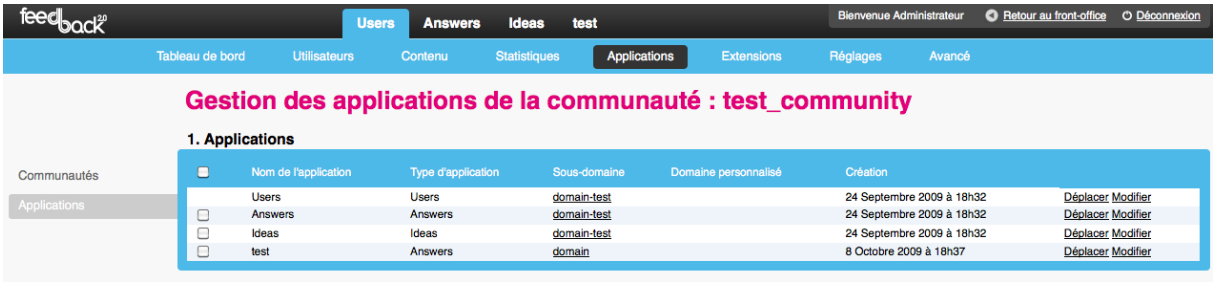
Dans le cas contraire il faut ajouter le paramètre « **charset** » dans l'url du SSO, en effet la fonction de hashage sha1 dépend de la représentation binaire des chaînes de caractères, et suivant l'encodage que vous utilisez les caractères accentués n'ont pas la même représentation. Nous vous offrons la possibilité de prendre en charge cette différence mais il faut l'indiquer dans le lien sso via le paramètre charset.

Le paramètre accepte les valeurs suivantes en fonction de votre encodage :

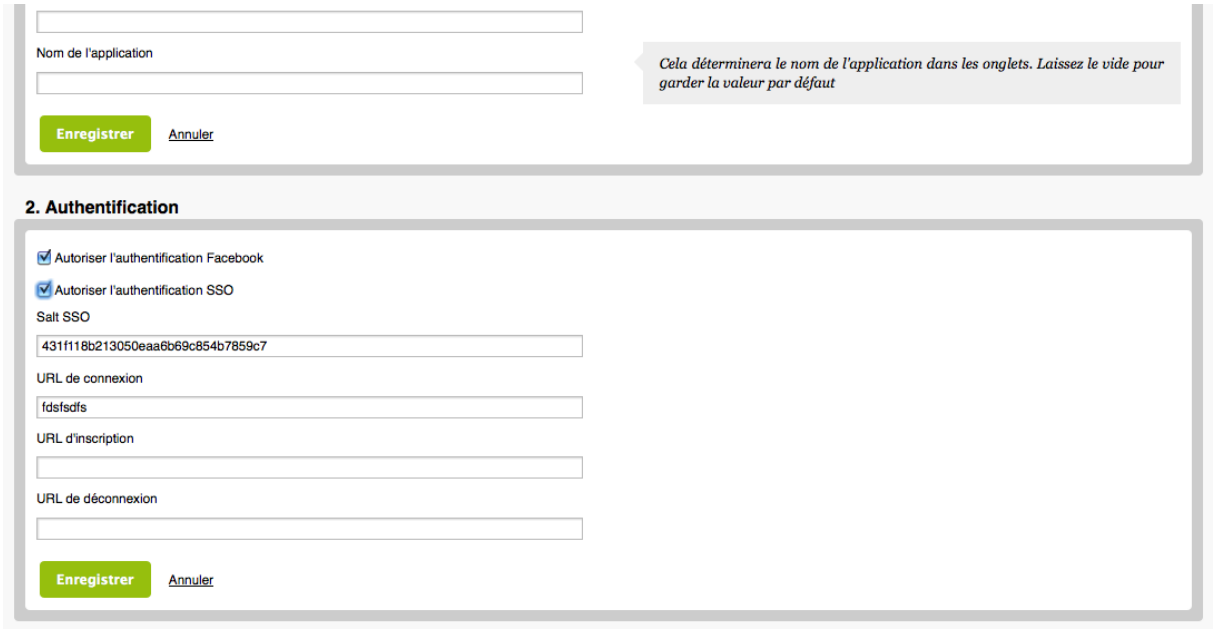
Valeur du paramètre charset	Nom standard de l'encodage	Informations
latin1	ISO-8859-1	Appelé aussi Western latin1.
latin15	ISO-8859-15	Latin1 étendue au caractères spéciaux européens comme le symbole « € »
winlatin1	CP1252	Dérivé du latin1 sur les plateformes Microsoft Windows

9. Configuration

Allez dans l'onglet **Applications**, puis cliquez sur le lien **modifier** de l'application.



Vous devriez avoir l'écran suivant :



Vous pourrez dès lors configurer certaines fonctionnalités.

- **URL de connexion** : URL sur laquelle l'utilisateur sera redirigé lors de l'authentification. Exemple, en cliquant sur le lien « S'identifier » sur l'application Feedback2.0. Un paramètre « **service** » représentant l'URL d'origine de l'utilisateur est automatiquement ajouté.

- **URL d'inscription** : URL sur laquelle l'utilisateur sera redirigé lors de l'inscription. Exemple, en cliquant sur le lien « s'inscrire » sur l'application Feedback 2.0. Un paramètre « **service** » représentant l'URL d'origine de l'utilisateur est automatiquement ajouté.

- **URL de déconnexion** : URL sur laquelle l'utilisateur sera redirigé lorsqu'il se déconnecte.