Authentic 2 - Development #28853

Plutôt que de demander le mot de passe lors d'une suppression, lancer une réauthentification

11 décembre 2018 12:12 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	11 décembre 2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Les méthodes d'authentification étant multiple demander le mot de passe pour la suppression d'un compte est contre-productive, à la place il faudrait demander une réauthentification si l'authentification est plus ancien qu'un certain seuil.

Le flowchart:
1. si GET
1.1. si dernière authentification < X minutes:
1.1.1. afficher un formulaire avec un jeton signé permettant le changement du mot de passe
2. si POST
1.2. sinon rediriger vers /login/?next=/accounts/delete/ avec un message indiquant pourquoi une ré-authentification est nécessaire
2.1. si le POST contient un jeton signé valide de moins de 10 minutes : supprimer le compte
2.2. sinon traiter comme un GET (aller en 1)

L'utilisation d'un jeton évite le problème d'un formulaire obtenu juste avant le dépassement du délai (la personne a alors 10 minutes pour compléter le formulaire).

Cas d'usage immédiate: personne connecté via FranceConnect voulant supprimer son compte

Demandes liées:

Lié à Authentic 2 - Development #61125: pouvoir s'authentifier de n'importe q...	**Fermé**	**26 janvier 2022**
Bloque Publik - Development #27081: Intégration cahier des charges FranceConnect	**Fermé**	**08 octobre 2018**

Révisions associées

Révision 8acfa99c - 21 février 2022 10:20 - Benjamin Dauvergne

admin: expose User.email_verified field (#28853)

Révision d8411870 - 21 février 2022 10:20 - Benjamin Dauvergne

misc: allow signed token to login view (#28853)

It prevents messing with the login view from unauthorized parties.

Révision 0423dbbb - 21 février 2022 10:47 - Benjamin Dauvergne

views: require authentication for deleting account without a verified email (#28853)

Historique

#1 - 11 décembre 2018 12:13 - Benjamin Dauvergne

- Bloque Development #27081: Intégration cahier des charges FranceConnect ajouté

#2 - 16 mai 2019 18:23 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#3 - 16 mai 2019 19:03 - Benjamin Dauvergne

- Fichier 0001-views-ask-for-reauthentication-when-deleting-account.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#4 - 17 mai 2019 09:47 - Benjamin Dauvergne

- Fichier 0001-views-ask-for-reauthentication-when-deleting-account.patch ajouté

Correction support Django 1.11 dans les tests.

#5 - 17 mai 2019 10:44 - Valentin Deniaud

DeleteAccountForm dans forms/profile.py peut être supprimé j'ai l'impression.

#6 - 17 mai 2019 11:03 - Benjamin Dauvergne

- Fichier 0001-views-ask-for-reauthentication-when-deleting-account.patch ajouté

Yep.

#7 - 17 juin 2019 16:53 - Valentin Deniaud

- Statut changé de Solution proposée à En cours

Il y a un %d orphelin (et il manque la traduction) :

```
1103                 messages.info(request,
1104                               _('Your last authentication is %d seconds old, '
1105                                 'you need to reauthenticate to delete your account'))
```

À part ça c'est bon pour moi. En passant, les lignes qui font plus de 100 caractères dans DeleteView gagneraient à être splittées.

Je note aussi que c'est dommage d'avoir perdu le préremplissage du nom d'utilisateur dans le formulaire de login, et que si il y a un moyen simple de le garder il faudrait y songer. Outre l'UX pas terrible, j'ai failli me faire avoir en testant : j'ai créé un nouvel utilisateur pour pouvoir le supprimer, je me suis connecté avec lui et j'ai demandé la suppression au bout d'une minute, et le formulaire de la page de réauthentification s'est affiché prérempli par FF avec mon compte de test habituel ; si je faisais pas gaffe, je supprimais le mauvais compte.

#8 - 17 juin 2019 16:56 - Frédéric Péters

```
1104                               _('Your last authentication is %d seconds old, '
1105                                 'you need to reauthenticate to delete your account'))
```

Plutôt parler aux gens dans des unités pertinentes ?

#9 - 17 juin 2019 19:58 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> Il y a un %d orphelin (et il manque la traduction) :
> [...]
>
> À part ça c'est bon pour moi. En passant, les lignes qui font plus de 100 caractères dans DeleteView gagneraient à être splittées.

J'applique une limite de 120.

> Je note aussi que c'est dommage d'avoir perdu le préremplissage du nom d'utilisateur dans le formulaire de login, et que si il y a un moyen simple de le garder il faudrait y songer. Outre l'UX pas terrible, j'ai failli me faire avoir en testant : j'ai créé un nouvel utilisateur pour pouvoir le supprimer, je me suis connecté avec lui et j'ai demandé la suppression au bout d'une minute, et le formulaire de la page de réauthentification s'est affiwché prérempli par FF avec mon compte de test habituel ; si je faisais pas gaffe, je supprimais le mauvais compte.

Il faut un POST pour supprimer un compte, si tu reviens de la vue de login la vue de suppression va se ré-afficher parce que tu viens via une redirection et donc un GET. Mais par contre c'est vrai qu'en cas d'erreur d'authent sur la vue de login le message parlant de la vue de suppression va partir; mais c'est un autre ticket et une vieille demande le fait d'avoir des messages persistant sur la page de login.

#10 - 17 juin 2019 19:59 - Benjamin Dauvergne

Les deux remarques prises en compte :

```
diff --git a/src/authentic2/views.py b/src/authentic2/views.py
index 3b46dcca..4d54da92 100644
--- a/src/authentic2/views.py
+++ b/src/authentic2/views.py
@@ -1101,7 +1101,7 @@ class DeleteView(FormView):
                return utils.redirect(request, request.path, params={'token': signer.sign(str(self.request.us
er.uuid))})
            else:
```

```
                messages.info(request,
-                               _('Your last authentication is %d seconds old, '
+                               _('Your last authentication is too old, '
                                  'you need to reauthenticate to delete your account'))
                return utils.login_require(request)
        return super(DeleteView, self).dispatch(request, *args, **kwargs)
```

#11 - 17 juin 2019 19:59 - Benjamin Dauvergne

- Fichier 0001-views-ask-for-reauthentication-when-deleting-account.patch ajouté

- Statut changé de En cours à Solution proposée

#12 - 18 juin 2019 10:44 - Valentin Deniaud

- Statut changé de Solution proposée à En cours

Je viens de penser que ce patch ne fait pas bon ménage avec le setting A2_LOGIN_REDIRECT_AUTHENTICATED_USERS_TO_HOMEPAGE. Si il est activé (pas le cas par défaut), impossible de supprimer son compte (sans avoir connaissance de la mécanique interne, sinon on se délogge/relogge et on va vite supprimer). C'est cette remarque qui te prive du ack, pas la suite.

Benjamin Dauvergne a écrit :

> Je note aussi que c'est dommage d'avoir perdu le préremplissage du nom d'utilisateur dans le formulaire de login, et que si il y a un moyen simple de le garder il faudrait y songer. Outre l'UX pas terrible, j'ai failli me faire avoir en testant : j'ai créé un nouvel utilisateur pour pouvoir le supprimer, je me suis connecté avec lui et j'ai demandé la suppression au bout d'une minute, et le formulaire de la page de réauthentification s'est affiwché prérempli par FF avec mon compte de test habituel ; si je faisais pas gaffe, je supprimais le mauvais compte.

Il faut un POST pour supprimer un compte, si tu reviens de la vue de login la vue de suppression va se ré-afficher parce que tu viens via une redirection et donc un GET. Mais par contre c'est vrai qu'en cas d'erreur d'authent sur la vue de login le message parlant de la vue de suppression va partir; mais c'est un autre ticket et une vieille demande le fait d'avoir des messages persistant sur la page de login.

Ce que je voulais dire c'est que dans le cas d'une authentification par login/mot de passe, le comportement d'avant qui était de simplement redemander le mdp est quand même plus agréable et cohérent que le comportement du patch où il faut réentrer son login (et via des cas limites comme celui que je citais, rien n'empêche de changer de login et donc de compte au moment de cette réauthentification).
Pour améliorer ça il faudrait que la vue de login comprenne que si l'utilisateur est déjà authentifié (ou en rendant ça explicite avec un paramètre GET), il faut ne permettre le login qu'à cet utilisateur (et préremplir + griser ou mieux, cacher comme avant le champ username). Mais c'est sûrement un casse-tête pour rendre ça générique à tous les plugins d'authent possibles.

#13 - 18 juin 2019 11:36 - Benjamin Dauvergne

Valentin Deniaud a écrit :

> Je viens de penser que ce patch ne fait pas bon ménage avec le setting A2_LOGIN_REDIRECT_AUTHENTICATED_USERS_TO_HOMEPAGE. Si il est activé (pas le cas par défaut), impossible de supprimer son compte (sans avoir connaissance de la mécanique interne, sinon on se délogge/relogge et on va vite supprimer). C'est cette remarque qui te prive du ack, pas la suite.

Hmm oui en plus ça impacte le CUT qui est le seul utilisateur de ce setting et ça me fait bien chier; réfléchissement Jean-Pierre...

> Benjamin Dauvergne a écrit :
>
> > Je note aussi que c'est dommage d'avoir perdu le préremplissage du nom d'utilisateur dans le formulaire de login, et que si il y a un moyen simple de le garder il faudrait y songer. Outre l'UX pas terrible, j'ai failli me faire avoir en testant : j'ai créé un nouvel utilisateur pour pouvoir le supprimer, je me suis connecté avec lui et j'ai demandé la suppression au bout d'une minute, et le formulaire de la page de réauthentification s'est affiwché prérempli par FF avec mon compte de test habituel ; si je faisais pas gaffe, je supprimais le mauvais compte.
>
> Il faut un POST pour supprimer un compte, si tu reviens de la vue de login la vue de suppression va se ré-afficher parce que tu viens via une redirection et donc un GET. Mais par contre c'est vrai qu'en cas d'erreur d'authent sur la vue de login le message parlant de la vue de suppression va partir; mais c'est un autre ticket et une vieille demande le fait d'avoir des messages persistant sur la page de login.
>
> Ce que je voulais dire c'est que dans le cas d'une authentification par login/mot de passe, le comportement d'avant qui était de simplement redemander le mdp est quand même plus agréable et cohérent que le comportement du patch où il faut réentrer son login (et via des cas limites comme celui que je citais, rien n'empêche de changer de login et donc de compte au moment de cette réauthentification).

Ok je comprends, mais je préférerai traiter ça dans un autre ticket :
1. parce que peu de gens suppriment leur compte, donc cette petite gêne n'est pas exagérée

2. ça rejoint un besoin plus large de login_hint[1] (jargon OIDC) où il est parfois possible de passer une indication sur l'identité de l'utilisateur; exemple en OIDC on peut mettre login_hint=<email> ou id_token_hint=<id_token> pour aider l'IdP à trouver l'utilisateur (en pré-remplissant le champ username, en redirigeant automatiquement vers un autre IdP s'il sait que c'est un utilisateur externe, en sélectionnant le bon compte si c'est un IdP gérant de multiple session en parallèle, voir google).

Mais dans le cas où l'utilisateur est déjà connecté je vais voir pour améliorer les choses.

[1] https://openid.net/specs/openid-connect-core-1_0.html#AuthRequest

> Pour améliorer ça il faudrait que la vue de login comprenne que si l'utilisateur est déjà authentifié (ou en rendant ça explicite avec un paramètre GET), il faut ne permettre le login qu'à cet utilisateur (et préremplir + griser ou mieux, cacher comme avant le champ username). Mais c'est sûrement un casse-tête pour rendre ça générique à tous les plugins d'authent possibles.

Je vais déjà pré-remplir et passer le focus sur le deuxième champ.

#14 - 18 juin 2019 12:05 - Benjamin Dauvergne

- Fichier 0002-views-ask-for-reauthentication-when-deleting-account.patch ajouté

- Fichier 0001-prefill-username-when-authenticated-28853.patch ajouté

- Statut changé de En cours à Solution proposée

Déjà le prefill du username.

#15 - 14 janvier 2020 11:09 - Valentin Deniaud

- Statut changé de Solution proposée à En cours

> réfléchissement Jean-Pierre

Ce ticket attend Jean-Pierre et non pas un ack comme dit dans https://dev.entrouvert.org/issues/38898#change-209609.

#16 - 26 janvier 2022 15:49 - Benjamin Dauvergne

- Lié à Development #61125: pouvoir s'authentifier de n'importe quelle manière pour un changement d'email ajouté

#17 - 26 janvier 2022 16:01 - Benjamin Dauvergne

- Fichier 0003-views-require-authentication-for-deleting-account-wi.patch ajouté

- Fichier 0002-misc-allow-signed-token-to-login-view-28853.patch ajouté

- Fichier 0001-admin-expose-User.email_verified-field-28853.patch ajouté

- Statut changé de En cours à Solution proposée

Je suis revenu sur ce ticket qui est devenu partiellement inutile via #27823 mais ça reste utile pour le cas où on a pas d'email vérifié, et l'infra déployé ici est réutilisée dans #61125.

#18 - 02 février 2022 15:47 - Paul Marillonnet

Première remarque, une ligne qui attise ma curiosité (je continue à relire le reste en attendant) :

```
    # Create blocks
    for authenticator in authenticators:
        if methods and not (authenticator.id in methods or set(authenticator.how) & set(methods)):
            continue
```

Pourquoi on en arrive à tester soit l'id de l'authentificateur ou bien son attribut how ? C'est l'existant sur GLC qui justifie de devoir tester les des deux à la fois ?
Je ne vois nulle part dans le code le cas où l'identifiant de l'authentificateur aurait été passé dans methods.

Edit : autre remarque sur une autre ligne qui m'interpelle, dans la nouvelle méthode AccountDeleteView.has_recent_authentication :

```
age = time.time() - utils_misc.last_authentication_event(request=self.request)['when']
```

si pour une raison ou une autre on ne retrouve pas d'événement pour la requête, genre des objets AuthenticationEvent manquants, alors

last_authentication_event renvoie @None et cette ligne va tracer.

#19 - 02 février 2022 16:44 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Première remarque, une ligne qui attise ma curiosité (je continue à relire le reste en attendant) :
> [...]
> Pourquoi on en arrive à tester soit l'id de l'authentificateur ou bien son attribut how ? C'est l'existant sur GLC qui justifie de devoir tester les des deux à la fois ?

Petit historique d'authentic et du patch: pour des raisons qui ont à voir avec SAML qui fait la différence (différence dont on se fout aujourd'hui) le mode "mot de passe" a deux valeurs pour "how" : password et password-on-https. Pour des raisons de bêtise ou de ticket que j'ai accepté sans réfléchir le module franceconnect a pour identifiant "fc" mais comme méthode "france-connect", pour simplifier j'ai fait id in method pendant l'écriture, puis ça marchait pas pour franceconnect donc j'ai ajouté method in self.hows puis après je me suis dit qu'on pourrait vouloir plusieurs méthode et c'est devenu ça.

Finalement ça ne marche pour authentic2_auth_saml où on peut condiérer que self.hows == [self.id] (y a pas de self.hows déclaré, vu que c'est toujours saml). Si tu trouves ça con, je rajoute un class SAMLAuthenticator\hows = ['saml'] et je vire la condition.

PS:

> Je ne vois nulle part dans le code le cas où l'identifiant de l'authentificateur aurait été passé dans methods.

Oui c'est dans les appels à misc_utils.login(...) la chaîne est généralement écrite directement.

#20 - 02 février 2022 19:27 - Frédéric Péters

> Pour des raisons de bêtise ou de ticket que j'ai accepté sans réfléchir le module franceconnect a pour identifiant "fc" mais comme méthode "france-connect",

Si jamais quelqu'un cherche ça arrive dans #21908 qui ajoute

```
+        data['authentication_method'] = 'france-connect'
```

dans le module qui a "fc" comme id.

#21 - 03 février 2022 17:32 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Petit historique d'authentic et du patch: pour des raisons qui ont à voir avec SAML qui fait la différence (différence dont on se fout aujourd'hui) le mode "mot de passe" a deux valeurs pour "how" : password et password-on-https. Pour des raisons de bêtise ou de ticket que j'ai accepté sans réfléchir le module franceconnect a pour identifiant "fc" mais comme méthode "france-connect", pour simplifier j'ai fait id in method pendant l'écriture, puis ça marchait pas pour franceconnect donc j'ai ajouté method in self.hows puis après je me suis dit qu'on pourrait vouloir plusieurs méthode et c'est devenu ça.

Merci pour l'historique et merci à Fred d'avoir identifié le ticket en question.

> Finalement ça ne marche pour authentic2_auth_saml où on peut condiérer que self.hows == [self.id] (y a pas de self.hows déclaré, vu que c'est toujours saml). Si tu trouves ça con, je rajoute un class SAMLAuthenticator\hows = ['saml'] et je vire la condition.

Oui je pense que ce serait mieux en virant cette condition.

#22 - 17 février 2022 19:39 - Benjamin Dauvergne

- Fichier 0003-views-require-authentication-for-deleting-account-wi.patch ajouté

- Fichier 0002-misc-allow-signed-token-to-login-view-28853.patch ajouté

- Fichier 0001-admin-expose-User.email_verified-field-28853.patch ajouté

Voilà, avec les modifs demandés (ce ticket est nécessaire pour pousser #61125).

#23 - 18 février 2022 20:34 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Ok, tout relu, ça me va. Juste une petite remarque de forme sur, dans 0003 :

```
            form.fields['password'].widget.attrs['autofocus'] = 'autofocus'
```

Il me semble que c'est juste évalué comme un booléen et on mettre juste = True à la place de cette chaîne (ça résulte en un <input type=… autofocus>, pas de valeur pour l'attribut autofocus).

Et juste un aparté pour dire qu'en effet attraper les ValueError lors du crypto.loads(token) me paraît justifié. Ça n'a pas l'air d'être le cas partout dans le code de a2, je vois des occurrences ici et là où il semblerait qu'il faille l'ajouter. Je vais regarder et créer un ticket si nécessaire.

#24 - 21 février 2022 10:26 - Benjamin Dauvergne

- Statut changé de Solution validée à Solution proposée

Paul Marillonnet a écrit :

> Et juste un aparté pour dire qu'en effet attraper les ValueError lors du crypto.loads(token) me paraît justifié. Ça n'a pas l'air d'être le cas partout dans le code de a2, je vois des occurrences ici et là où il semblerait qu'il faille l'ajouter. Je vais regarder et créer un ticket si nécessaire.

J'ai modifié la partie autofocus pour prendre en compte ta remarque et les dernières modifications de Fred sur le sujet, la branche est à jour (seul le dernier commit est concerné).

#25 - 21 février 2022 10:48 - Benjamin Dauvergne

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

```
commit 0423dbbbcac652f3d18181e0835a43c23a520db0
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Jun 18 12:05:09 2019 +0200

    views: require authentication for deleting account without a verified email (#28853)

commit d8411870c2f041b7c3ba7cace1b907576989ae79
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Jan 26 10:25:48 2022 +0100

    misc: allow signed token to login view (#28853)

    It prevents messing with the login view from unauthorized parties.

commit 8acfa99cc2dc2d71bd1ca6696343c51fdd1f888b
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Jan 26 11:19:03 2022 +0100

    admin: expose User.email_verified field (#28853)
```

#26 - 22 février 2022 15:17 - Transition automatique

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

#27 - 24 avril 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-views-ask-for-reauthentication-when-deleting-account.patch	5,64 ko	16 mai 2019	Benjamin Dauvergne
0001-views-ask-for-reauthentication-when-deleting-account.patch	5,99 ko	17 mai 2019	Benjamin Dauvergne
0001-views-ask-for-reauthentication-when-deleting-account.patch	6,93 ko	17 mai 2019	Benjamin Dauvergne
0001-views-ask-for-reauthentication-when-deleting-account.patch	6,92 ko	17 juin 2019	Benjamin Dauvergne
0002-views-ask-for-reauthentication-when-deleting-account.patch	6,92 ko	18 juin 2019	Benjamin Dauvergne
0001-prefill-username-when-authenticated-28853.patch	1,21 ko	18 juin 2019	Benjamin Dauvergne
0003-views-require-authentication-for-deleting-account-wi.patch	24,7 ko	26 janvier 2022	Benjamin Dauvergne
0002-misc-allow-signed-token-to-login-view-28853.patch	1,4 ko	26 janvier 2022	Benjamin Dauvergne
0001-admin-expose-User.email_verified-field-28853.patch	1,62 ko	26 janvier 2022	Benjamin Dauvergne
0003-views-require-authentication-for-deleting-account-wi.patch	25,6 ko	17 février 2022	Benjamin Dauvergne
0002-misc-allow-signed-token-to-login-view-28853.patch	1,35 ko	17 février 2022	Benjamin Dauvergne

0001-admin-expose-User.email_verified-field-28853.patch	1,62 ko	17 février 2022	Benjamin Dauvergne