Comment paramétrer la politique de gestion des mots de passe ?

Cet écran va vous permettre de paramétrer les sécurités d'accès à l'application.

Rendez-vous sur l'écran de paramétrage : **Paramétrage > Général > Paramètres > Sécurité**

L'ensemble des paramètres à votre disposition vous sont détaillés ci-après. Une fois renseignés et enregistrés, ils constitueront la sécurité d'accès à votre instance.

Adresse de l'expéditeur :
Ne pas modifier ce champ : il s'agit de l'adresse depuis laquelle les notifications par email vous seront adressées.

Test de complexité du mot de passe :
Ce champ permet de définir le degré de complexité et la longueur du mot de passe lorsque vos utilisateurs s'authentifient par le biais du système d'authentification interne d'oHRis.
Vous pouvez imposer la présence de chiffres, lettres, caractères spéciaux, etc. associée à une longueur minimale. Ce contrôle est réalisé lorsqu'un utilisateur change son mot de passe oHRis.
La CNIL a formulé une nouvelle recommandation le 17 octobre 2022 sur la gestion des mots de passe (https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite) et a proposé notamment ces 2 exemples :
Exemple 1 : au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles
Exemple 2 : au minimum 14 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire

Une expression régulière (ou « regex ») doit être intégrée dans ce champ :
Pour l'exemple 1, vous devez paramétrer :

```
^(?=.*[&é~»#'{|è`_\ç^à@)+=}^(£$%ù*µ,?;.:\/!§-])(?=.*[0-9])(?=.*[a-
z])(?=.*[A-Z])(.{12,})$
```

Pour l'exemple 2, vous devez paramétrer :

```
^(?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])(.{14,})$
```

Nombre de tentatives de connexion avant blocage :
oHRis est capable de bloquer un compte utilisateur après un nombre limité d'échecs d'authentification pour un même identifiant (Votre compte oHRis est bloqué ?). Ce système est un premier rempart à une attaque informatique qui consisterait à tester successivement de nombreux mots de passe (attaque dite par force brute).
Si vous paramétrer la valeur « 5 », cela signifie qu'un utilisateur a jusqu'à 5 tentatives d'authentification ; autrement dit, s'il a oublié son mot de passe, il a jusqu'à 5 essais.

Durée du blocage après plusieurs tentatives de connexion en échec (en minutes) :

Le compte utilisateur pour lequel il y a eu dépassement du nombre de tentatives infructueuses de connexion est bloqué pendant X minutes.
Si vous paramétrez la valeur « 10 », cela signifie que l'utilisateur devra attendre 10 minutes avant de renouveler sa tentative de connexion à oHRis.
Un message en rouge à l'écran indique à l'utilisateur que son compte est bloqué. Un gestionnaire ou un administrateur peut néanmoins débloquer son compte en suivant la procédure Comment débloquer le compte d'un utilisateur ?.

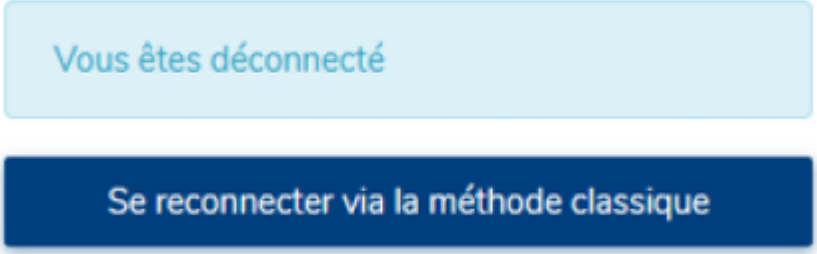
Description du mot de passe attendu :
Ce champ permet de décrire les critères de complexité et de longueur imposés aux utilisateurs. Si un utilisateur tente de modifier son mot de passe et que ce dernier n'est pas conforme aux critères définis dans "Test de complexité du mot de passe", le message que vous paramétrez dans ce champ s'affiche à l'écran.
Pour l'exemple 1, vous pouvez paramétrer « 12 caractères minimum, dont au moins une majuscule, une minuscule, un chiffre et un caractère spécial »
Pour l'exemple 2, vous pouvez paramétrer « 14 caractères minimum dont au moins une majuscule, une minuscule et un chiffre »

Nombre de jours avant demande de changement de mot de passe : oHRis permet de mettre en place une politique d'expiration des mots de passe. Les utilisateurs sont alors obligés de changer leur mot de passe à une certaine fréquence.
Si vous paramétrez la valeur « 60 », ils doivent changer leur mot de passe tous les 60 jours.
Si vous paramétrez « 0 », aucune expiration n'est en place.

Désactiver la réinitialisation du mot de passe :
Ce paramètre a pour effet d'interdire le changement de mot de passe sur l'écran d'authentification d'oHRis. L'utilisateur visualise tout de même le lien "Mot de passe oublié" mais s'il clique dessus, un message bloquant s'affiche.
Ce paramètre est à activer lorsqu'un mode d'authentification externe est utilisé.

Message à afficher si la réinitialisation du mot de passe est désactivée :
Il s'agit ici du message bloquant à paramétrer dans le cas où la fonctionnalité de réinitialisation du mot de passe est désactivée.
Vous pouvez par exemple indiquer : Votre mot de passe n'est pas stocké dans oHRis. Veuillez réinitialiser votre mot de passe depuis [indiquer le nom du logiciel/système]

Désactiver la possibilité de reconnexion interne après une déconnexion :
Ce paramètre est à activer lorsqu'un mode d'authentification externe est utilisé.
Lorsqu'un utilisateur se déconnecte d'oHRis, il n'est donc pas redirigé vers la mire d'authentification d'oHRis mais vers une page affichant ce message :



L'utilisateur peut alors cliquer sur “Se reconnecter via la méthode classique” et est redirigé vers le mode d'authentification externe.

Activer l'authentification double facteur :
Les éléments détaillés vous sont repris sur cette page : Comment paramétrer l'authentification double facteur ?

Et enfin, enregistrez en bas de page.