Comment paramétrer l'authentification double facteur ?

L'**authentification double facteur** permet de renforcer la sécurité de l'accès à notre application grâce à l'ajout d'un second facteur d'authentification.

Lors de la connexion, si le mode d'authentification est celui d'oHRis, alors une fois que l'utilisateur a saisi un mot de passe valide, il arrive sur l'écran de double authentification et un code lui est demandé. Il reçoit alors un code unique par email (ce code est valable 10 minutes).

Si il active la coche "Se souvenir de cet appareil", l'utilisateur a la possibilité de se connecter pendant 30 jours avant qu'un nouveau contrôle d'authentification soit effectué.

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

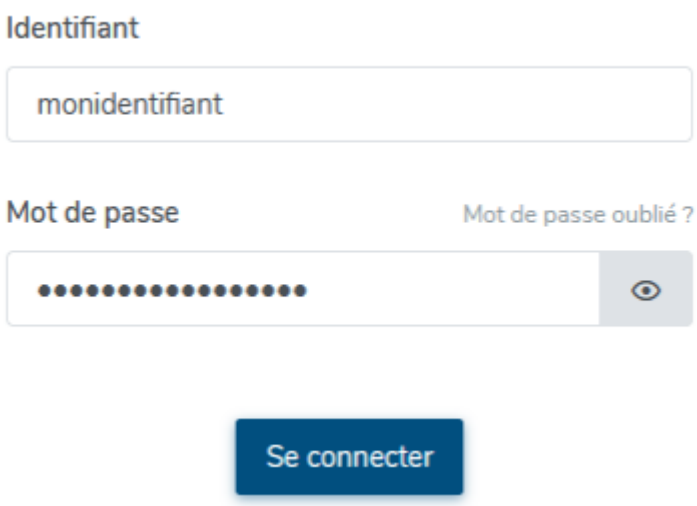
En bas de page, vous disposez du champ **Activer l'authentification double facteur** que vous pouvez cocher pour activer la fonctionnalité.
Puis enregistrez.

Depuis septembre 2023, lors de la création d'une nouvelle instance, ce paramètre est activé par défaut.

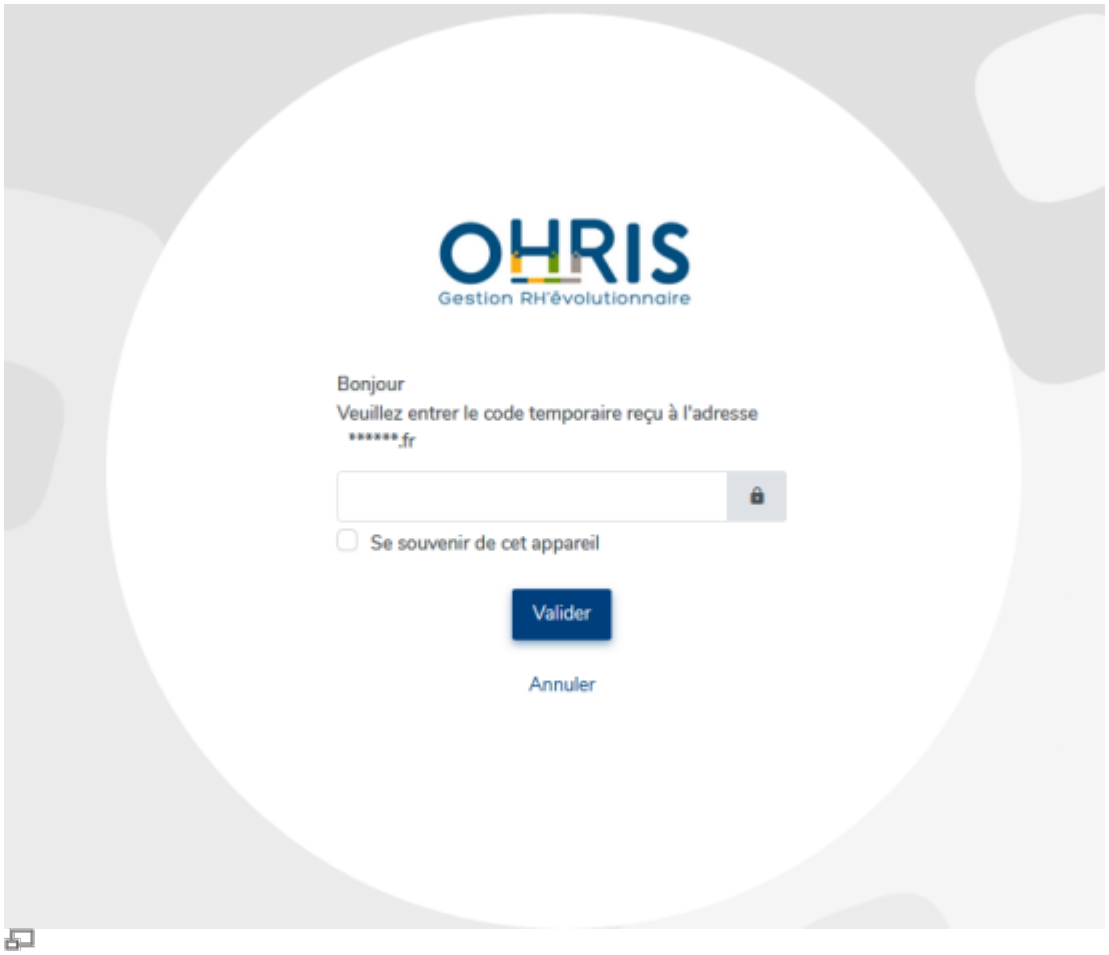
> En cas de saisie d'un mot de passe erroné, alors peu importe le nombre d'authentifications "de confiance" réalisées, le système redemandera un code à usage unique.

Dans la pratique côté utilisateur :

Une fois le paramétrage activé, l'utilisateur va se connecter à l'application comme habituellement :



Et lors de sa validation, un nouvel écran va s'afficher :



L'utilisateur reçoit par mail le code demandé (valable 10 minutes) :

Une fois le code renseigné, la connexion “de confiance” à l'application s'effectue.
Et si la coche “**Se souvenir de cet appareil**” est activée, alors cette connexion “de confiance” sera valable pendant 30 jours.

Cette connexion de confiance est valable 30 jours sur le même appareil, le même navigateur et si il n'y a pas de nettoyage des cookies. Sinon, une nouvelle authentification via code à usage unique

sera nécessaire.

Il est également possible de choisir que la double authentification s'effectue par une application TOTP.

En tant qu'administrateur ou gestionnaire, il est possible de désactiver la double authentification par application TOTP depuis la rubrique *Connexion* de la fiche utilisateur.

Une page détaillée sur le paramétrage de la politique de gestion des mots de passe est à votre disposition.