Est-il possible d'utiliser l'authentification SSO pour se connecter à Opentime ?

Nous utilisons depuis peu Microsoft Azure Active Directory (Azure AD) dans notre structure pour centraliser la gestion des identités et des accès. Nous aimerions intégrer notre instance d'Opentime à Azure pour que les salariés se connectent via SSO. Est-ce possible ?

Opentime est **bien compatible avec le Single Sign-On (SSO) via le protocole SAML**. Cette intégration permet à vos collaborateurs de se connecter à Opentime à l'aide de leurs identifiants d'entreprise pour simplifier la gestion des accès.

Quels sont les avantages du SSO ?

En intégrant Opentime à votre système d'authentification, vos collaborateurs se connectent au logiciel **avec les mêmes identifiants qu'ils utilisent pour d'autres applications**, réduisant ainsi le nombre de mots de passe à gérer. Ils n'ont plus besoin de se reconnecter chaque fois qu'ils accèdent à Opentime, ce qui simplifie leur saisie du temps.

Le SSO **renforce aussi la sécurité de vos données** en réduisant le risque d'utilisation de mots de passe faibles ou partagés.

Comment intégrer Opentime à votre système d'authentification unique SSO ?

Opentime **prend en charge tout fournisseur d'identité (IDP) compatible SAML, comme Okta, Microsoft Azure, Google Workspace**, et d'autres solutions SSO conformes à ce standard.

Pour activer le SSO sur Opentime, nous vous invitons à contacter notre équipe via le formulaire de contact ou à nous appeler au numéro **03 20 06 51 26**. Nous aurons besoin de quelques informations techniques pour effectuer l'intégration et nous pourrons travailler en collaboration avec votre équipe IT.

Pas d'inquiétude, ce paramétrage **peut être réalisé rapidement et sans frais supplémentaires** : il est inclus dans votre abonnement Opentime (à l'exception des abonnements freemium).

Extrait de l'aide en ligne du site Opentime.fr

Pour plus d'infos, contactez l'équipe Opentime à support@opentime.net ou au 03 20 06 51 26