VISIATIV DOCUMENT

Version 2.3

Guide de configuration SSO

Sommaire

La documentation

En cas de problème...

Si vous vous trouvez confronté à un problème qui ne trouve pas de solution dans ce guide, Visiativ met à votre disposition plusieurs outils, complémentaires à la documentation, pour vous permettre de trouver rapidement une réponse à vos questions.

Support technique - Le site MyMoovapps

Dans le cadre du contrat de maintenance Visiativ, vous disposez d'un compte utilisateur sur notre site MyMoovapps, à l'adresse suivante : https://www.mymoovapps.net

Remarque - Si vous n'avez pas encore de compte, vous pouvez en faire la demande : rendez-vous sur la page d'accueil du site et suivez les instructions pour vous inscrire.

Les éléments suivants sont à votre disposition sur le site :

- **Base de connaissance** : recherchez d'abord dans la base de connaissance si, parmi les nombreux articles techniques régulièrement publiés, certains peuvent vous aider à résoudre votre problème.
- **Forums** : ensuite, si votre problème porte sur l'utilisation du produit ou sur une adaptation que vous souhaitez réaliser, utilisez les forums. Ils vous permettront de dialoguer en ligne avec les équipes de développement et les autres utilisateurs.
- **Support en ligne** : enfin, pour un problème bloquant et urgent, utilisez le support en ligne en soumettant une demande à la hotline.

Formations et prestations complémentaires

Visiativ et ses partenaires offrent des formations à l'utilisation du logiciel, ainsi que des prestations complémentaires. N'hésitez pas à nous contacter pour plus de détails.

Paramétrage SSO

Les points abordés sont les suivants :

Paramétrage du SSO pour le client riche Visiativ Document

Prérequis

- Un tenant Team (fournisseur d'identité **OpenID Connect**).
- Un tenant Process (permettant la synchro d'annuaire).
- Un tenant Document.
- Les utilisateurs concernés par le SSO devront être créés par synchro depuis Process qui est l'annuaire maître.

  ```
  cf. https://sso.doc.moovapps.com/fr/synchronisation/master/
  ```

  Il faudra paramétrer :

  1. Le connecteur de synchro d'annuaire Process vers Document, voir doc du RC : « Add-on Visiativ Document - Visiativ Process ».

     ```
     cf. dernière version Add-on Visiativ Document - Visiativ Process
     ```

  2. Le connecteur de synchro d'annuaire Process vers Team :

     ```
     cf. https://sso.doc.moovapps.com/fr/cases/process/
     ```

Références

Toutes les informations techniques concernant le SSO Visiativ se trouve dans le lien :
https://sso.doc.moovapps.com

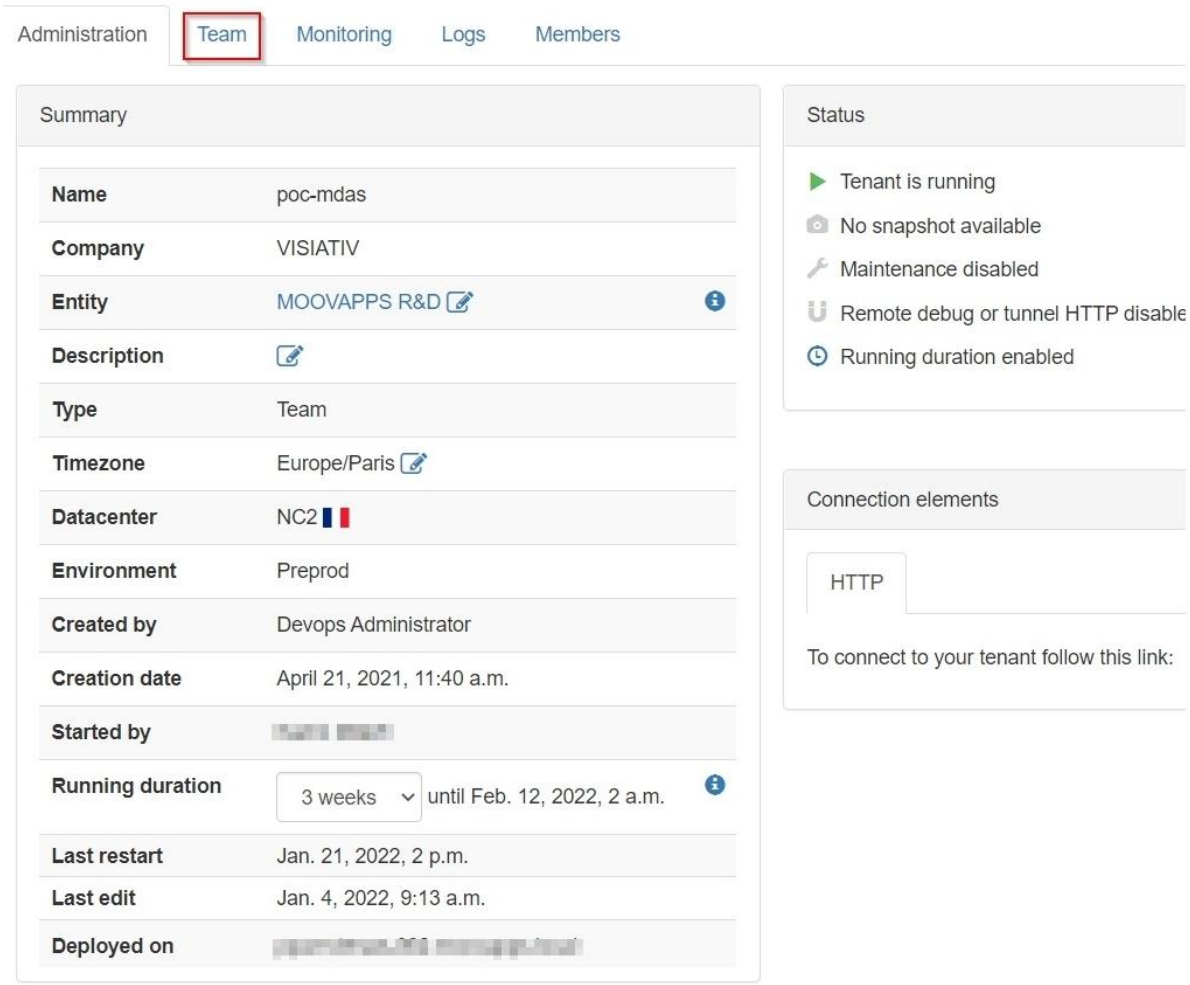
La documentation SSO de Document est également disponible avec le lien ci-dessous :
https://sso.doc.moovapps.com/fr/cases/document/

Paramétrer le serveur d'authentification (Visiativ SSO)

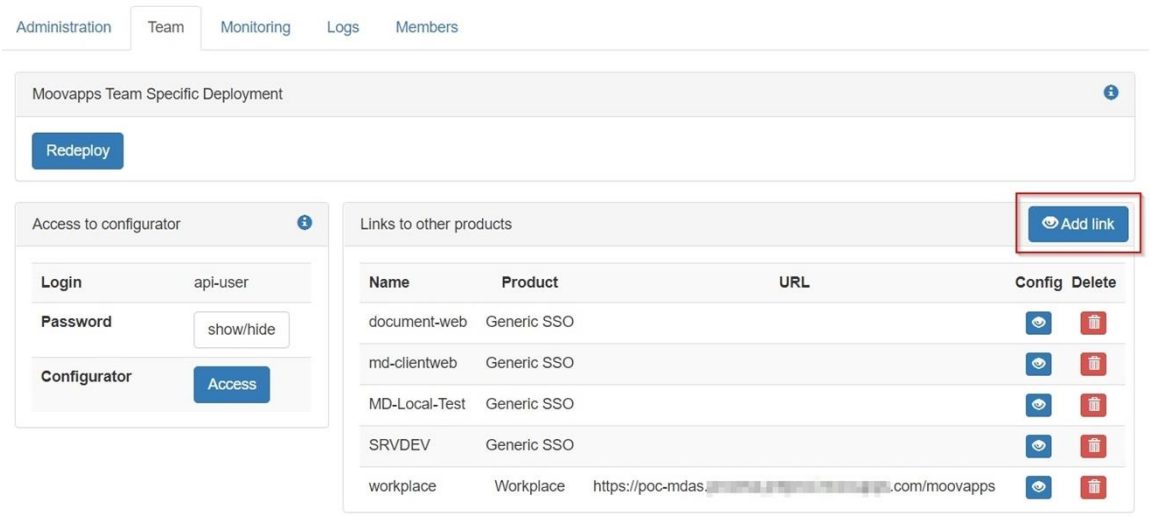
Si vous n'avez pas en votre possession l'identifiant « **client_id** » et le mot de passe « **client_secret** » de votre client **OpenID Connect**, il vous faudra les générer depuis le « cloud manager » en suivant la procédure indiquée ci-dessous.

Pour paramétrer le serveur d'authentification

1. Depuis Visiativ Cloud Manager, allez sur votre tenant Team, cliquez sur l'onglet **Team**



2. Pour ajouter une config SSO d'application Document, cliquez sur **Add link**.

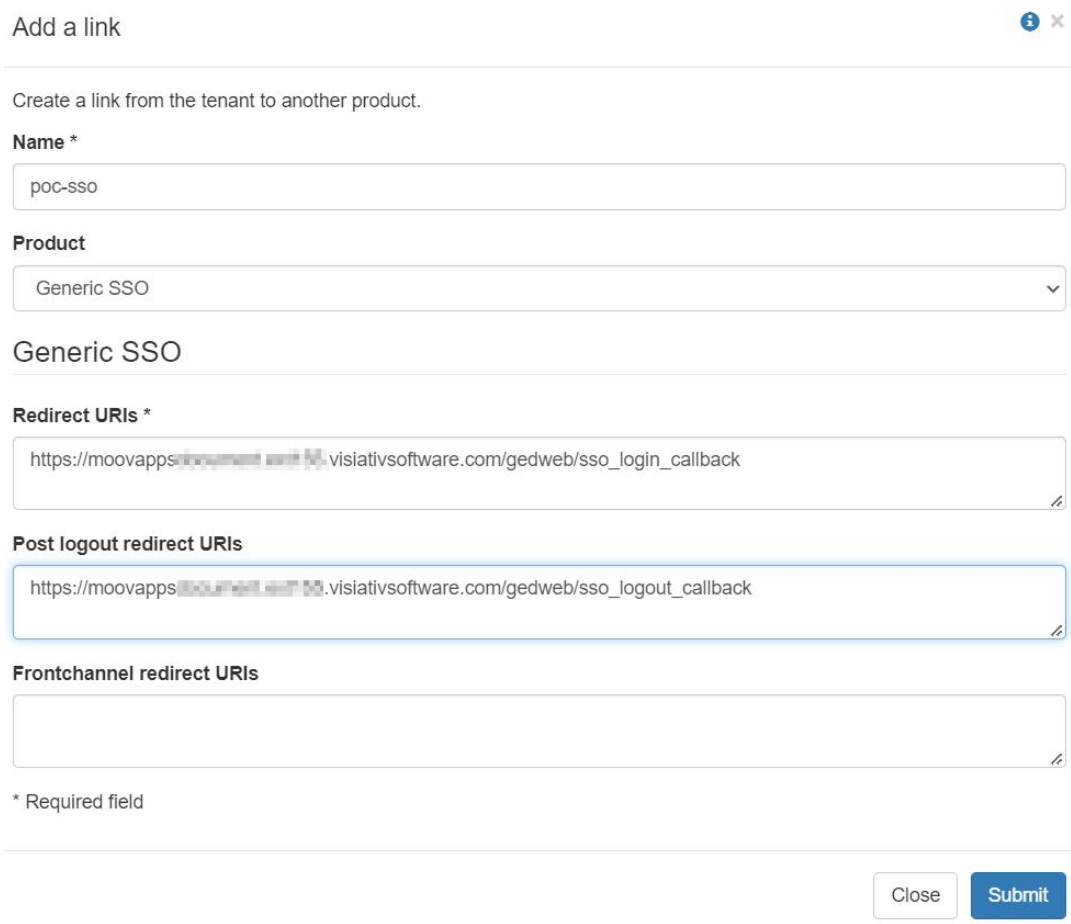


3. Sélectionnez l'option « **Generic SSO** » et saisissez :
   - Un nom
   - Les URLs de redirection autorisées sous la forme :
     - racine_du_serveur_md/gedweb/sso_login_callback
   - Les URLs de déconnexion autorisées sous la forme :
     - racine_du_serveur_md/gedweb/sso_logout_callback

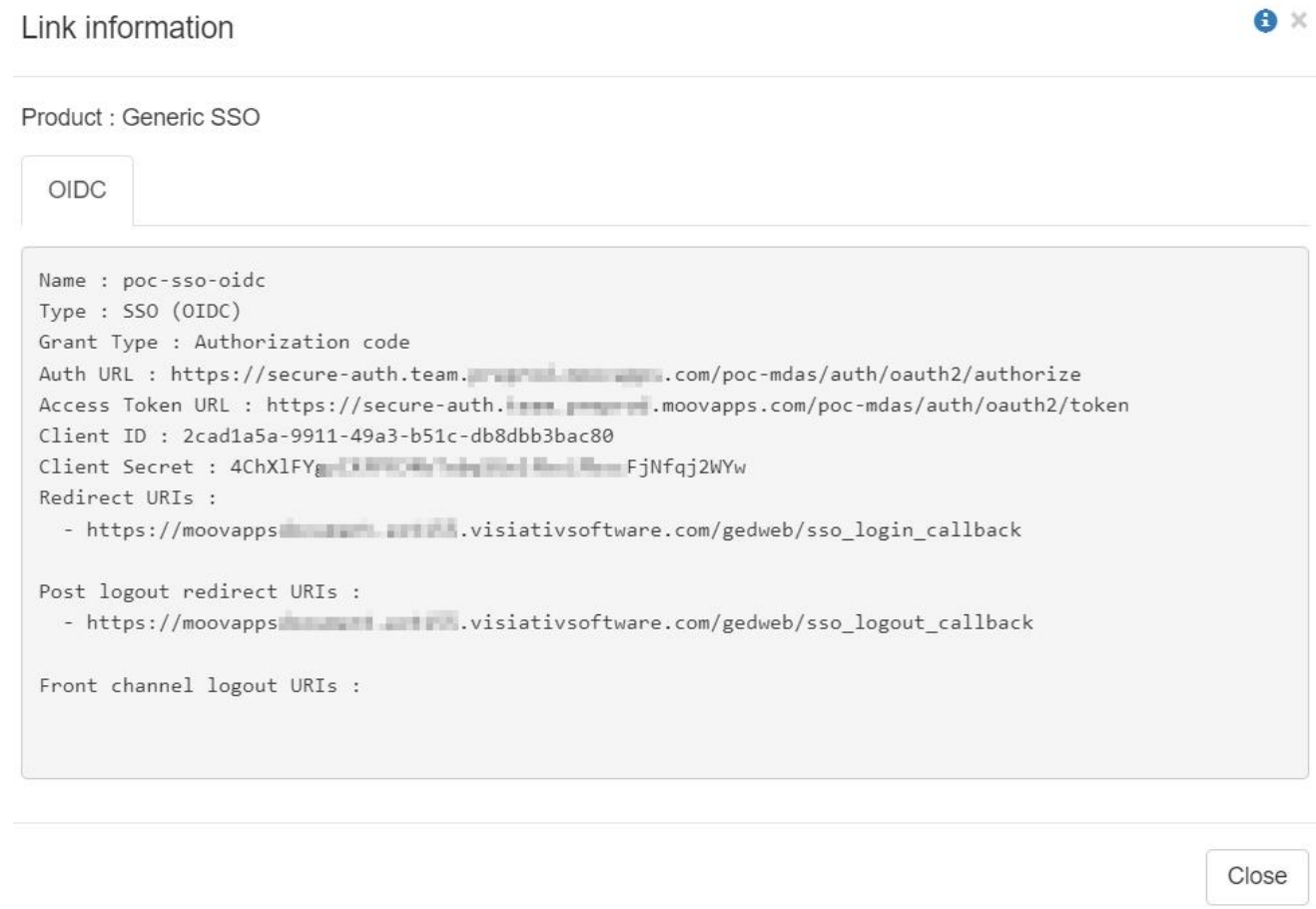
Créer une configuration acceptant le protocole https

***Remarque** - Il fortement déconseillé de passer par le protocole http ou mélanger du protocole http et https.*

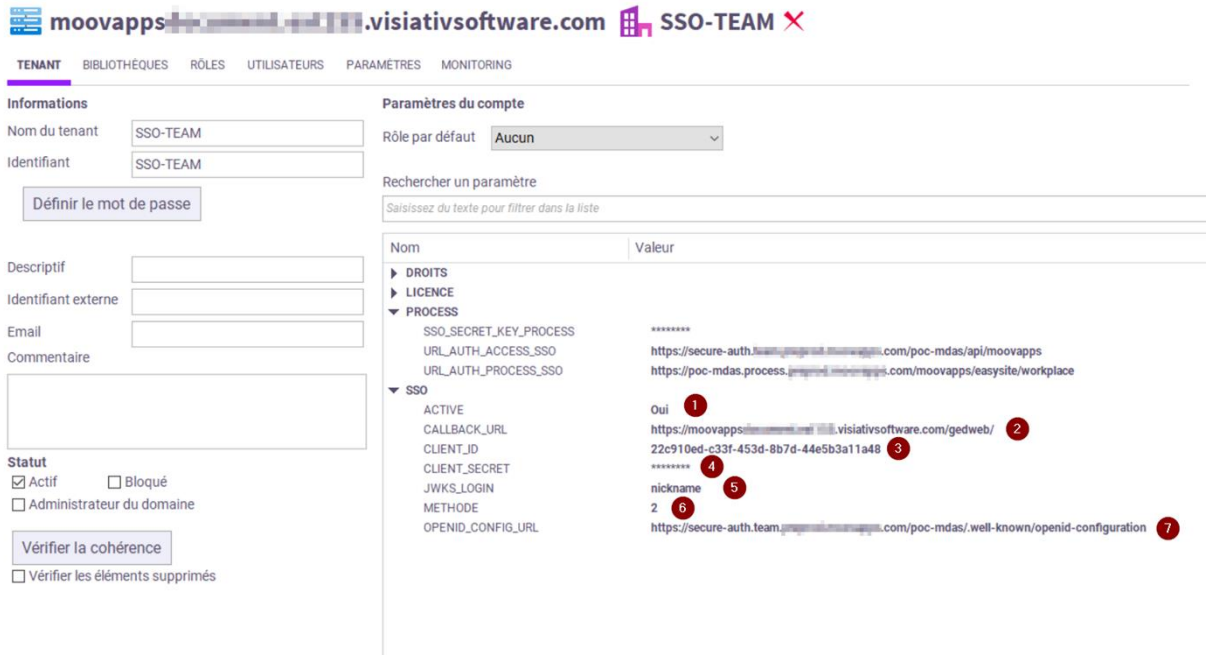
Exemple de configuration https :



4. Validez la configuration en cliquant sur le bouton **Submit**.
5. Récupérez le **Client ID** et le **Client Secret** de l'application SSO qui seront utilisés par la suite dans le serveur Visiativ Document, voir Paramétrer le serveur Visiativ Document, p. 12.



Paramétrer le serveur Visiativ Document



Pour paramétrer le serveur Visiativ Document

1. Connectez-vous en tant qu'administrateur du tenant.
2. Dans la section SSO, ajoutez les clés suivantes :
   - **ACTIVE** : active ou pas l'authentification SSO pour tout le tenant.
   - **CALLBACK_URL** : Racine de l'URL + suffixe « **/gedweb** », redirection autorisée par le serveur d'authentification SSO. Le serveur MDAS se chargera d'ajouter les suffixes « **sso_login_callback** » et « **sso_logout_callback** ».
   - **CLIENT_ID** : Renseigner l'identification de l'application obtenue dans Team.
   - **CLIENT_SECRET** : Renseigner la clé secrète de l'application obtenue dans Team. La clé une fois saisie dans MD ne sera plus lisible.
   - **JWKS_LOGIN** : Permet de récupérer le login SSO via le Jwks.
     En fonction du serveur d'authentification, la valeur est différente :
     - Avec Team, la valeur est : nickname,
     - Avec identity, la valeur est : preferred_username.
   - **METHODE** : L'authentification SSO devant passer par un navigateur web, il est possible de choisir :
     - L'utilisation du navigateur par défaut Windows (option 2) ;
     - Le navigateur intégré (option 1).
   - **OPENID_CONFIG_URL** : Saisissez l'URL « **discovery OpenID Connect** » du tenant SSO TEAM.

   L'URL devra être de la forme :

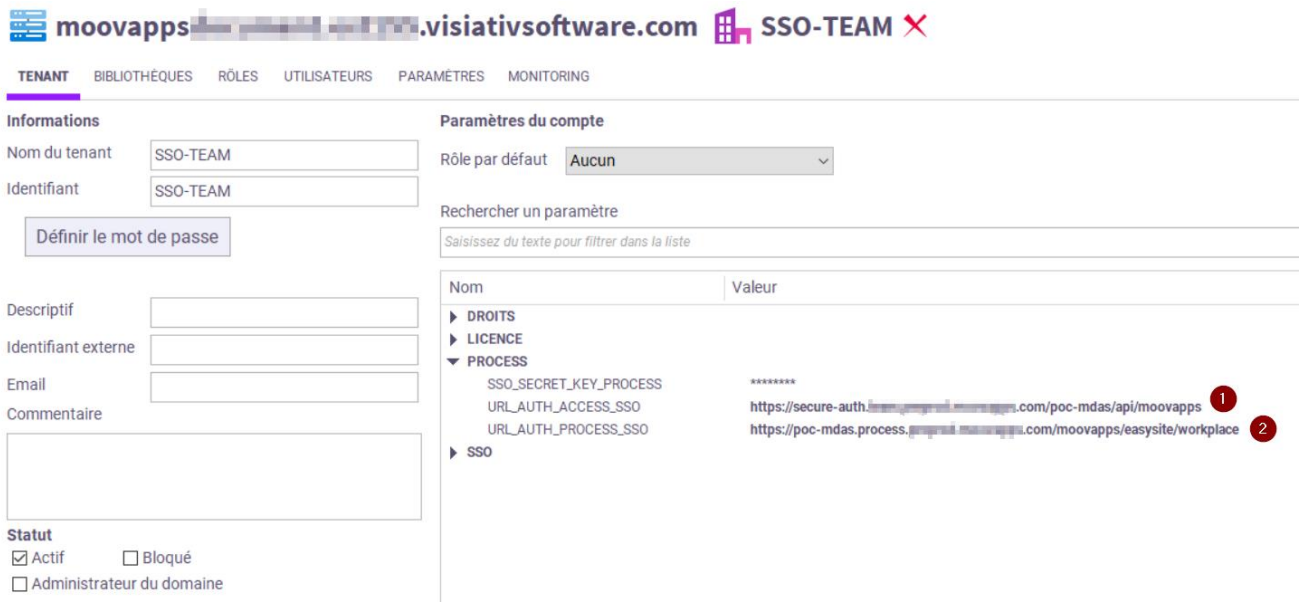
   ```
   https://<serveur_sso>/<tenant>/.well-known/openid-configuration
   ```

Configurations possibles des connexions entre Visiativ Document et Process

Pour paramétrer le serveur Visiativ Document avec Process plusieurs configurations sont possibles

	Tenant Process en SSO	**Tenant Process NON SSO**
	Uniquement de la publication	Pour de l'authentification et/ou de la publication
Tenant Visiativ Document en SSO **Prérequis** : - CLEE SSO\ACTIVE = OUI - Utilisateur ged de type « Visiativ Process »	- Authentification avec serveur d'authentification SSO (Team ou Identity) - La publication utilisera les clés : PROCESS\URL_AUTH_ACCESS_SSO PROCESS\URL_AUTH_PROCESS_SSO	Configuration Impossible (Pas de mode hybride)
Tenant Visiativ Document NON SSO **Prérequis** : - CLEE SSO\ACTIVE = NON ou clé Inexistante - Utilisateur ged de type « Visiativ Process »	Configuration Impossible (Pas de mode hybride)	- Utilisation de Process comme serveur maitre d'authentification. - L'authentification et/ou la publication utilisera la clé : PROCESS\URL_AUTH_PROCESS

L'utilisation du connecteur Process nécessite le paramétrage de clés se trouvant dans la section « PROCESS ».



1. PROCESS\URL_AUTH_ACCESS_SSO

   Lors de la Publication SSO, pour communiquer avec Process, les serveurs d'authentification Team et Identity n'utilisent pas là même architecture. Team utilise une Gateway pour communiquer avec Process mais pas Identity, ce qui change la structure des API.

   Pour une config avec Identity, on aura une URL de la forme :

   ```
   https://<nom_du_tenant>.process.moovapps.com/moovapps/navigation
   ```

   <nom_du_tenant> représente le nom du tenant

   Si par exemple le tenant qui a été créé est « poc-mdas », nous aurons comme url

   ```
   https://poc-mdas.process.moovapps.com/moovapps/navigation
   ```

   Pour une config avec Team, on aura une URL de la forme :

   ```
   https://secure-auth.team.moovapps.com/<nom_du_tenant>/api/moovapps
   ```

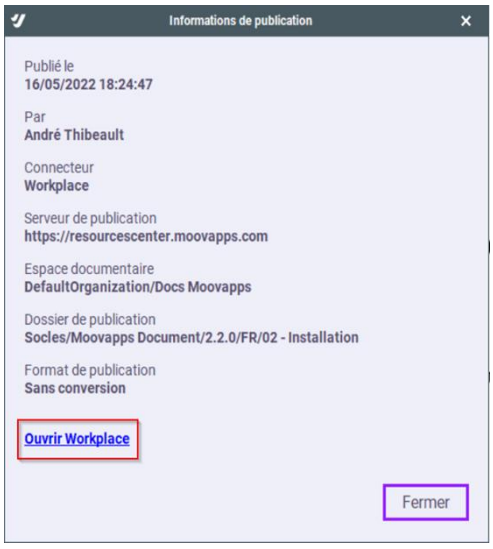
   <nom_du_tenant> représente le nom du tenant

   Si par exemple le tenant qui a été créé est « poc-mdas », nous aurons comme url

   ```
   https://secure-auth.team.moovapps.com/poc-mdas/api/moovapps
   ```

2. PROCESS\URL_AUTH_PROCESS_SSO

   Cette clé a pour unique fonction d'ouvrir l'espace de navigation Process à partir du panneau d'information.

   La valeur de l'url est de la forme :

   ```
   https://<nom_du_serveur_process>/moovapps/easysite/workplace
   ```

   L'utilisation de cette clé nécessite que votre serveur Process soit correctement configuré en mode SSO.

   Référez-vous à la documentation de paramétrage SSO de Process :

   ```
   https://sso.doc.moovapps.com/fr/cases/process/
   ```

Information

La clé `PROCESS\URL_AUTH_PROCESS` est uniquement utilisée dans un contexte sans SSO. Pour du SSO, dans la section PROCESS n'utiliser que les clés ayant références au SSO `PROCESS\URL_AUTH_PROCESS_SSO et PROCESS\URL_AUTH_ACCESS_SSO`