

VISIATIV DOCUMENT

Version 2025

Guide de configuration SSO

Copyright © 2024 Visiativ. Tous droits réservés.

Ce manuel, de même que le logiciel dont il traite, est cédé sous licence et ne peut être copié ou utilisé que conformément à la licence. Les informations contenues dans ce manuel sont données à titre purement indicatif.

Elles peuvent être modifiées sans préavis et ne constituent pas un engagement de la part de Visiativ. Visiativ dégage toute responsabilité vis-à-vis des erreurs ou imprécisions qui pourraient être relevées dans ce manuel.

Les modèles de documents fournis dans ce produit le sont à titre d'exemple et d'aide. Visiativ se dégage de toute responsabilité dans les conséquences de leur utilisation.

Sauf autorisation spécifiée dans la licence, aucune partie de ce manuel ne peut être reproduite, enregistrée ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, ou autre, sans l'autorisation écrite préalable de Visiativ.

Sommaire

Sommaire	3
La documentation	4
<hr/>	
En cas de problème... ..	5
Paramétrage SSO	6
<hr/>	
Paramétrage du SSO pour le client riche Visiativ Document	7
Prérequis.....	7
Paramétrer le serveur d’authentification (Visiativ SSO).....	8
Paramétrer le serveur Visiativ Document	12
Configurations possibles des connexions entre Visiativ Document et Process	14

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, p. 7
- Configurations possibles des connexions entre Visiativ Document et Process, p. 14

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 :

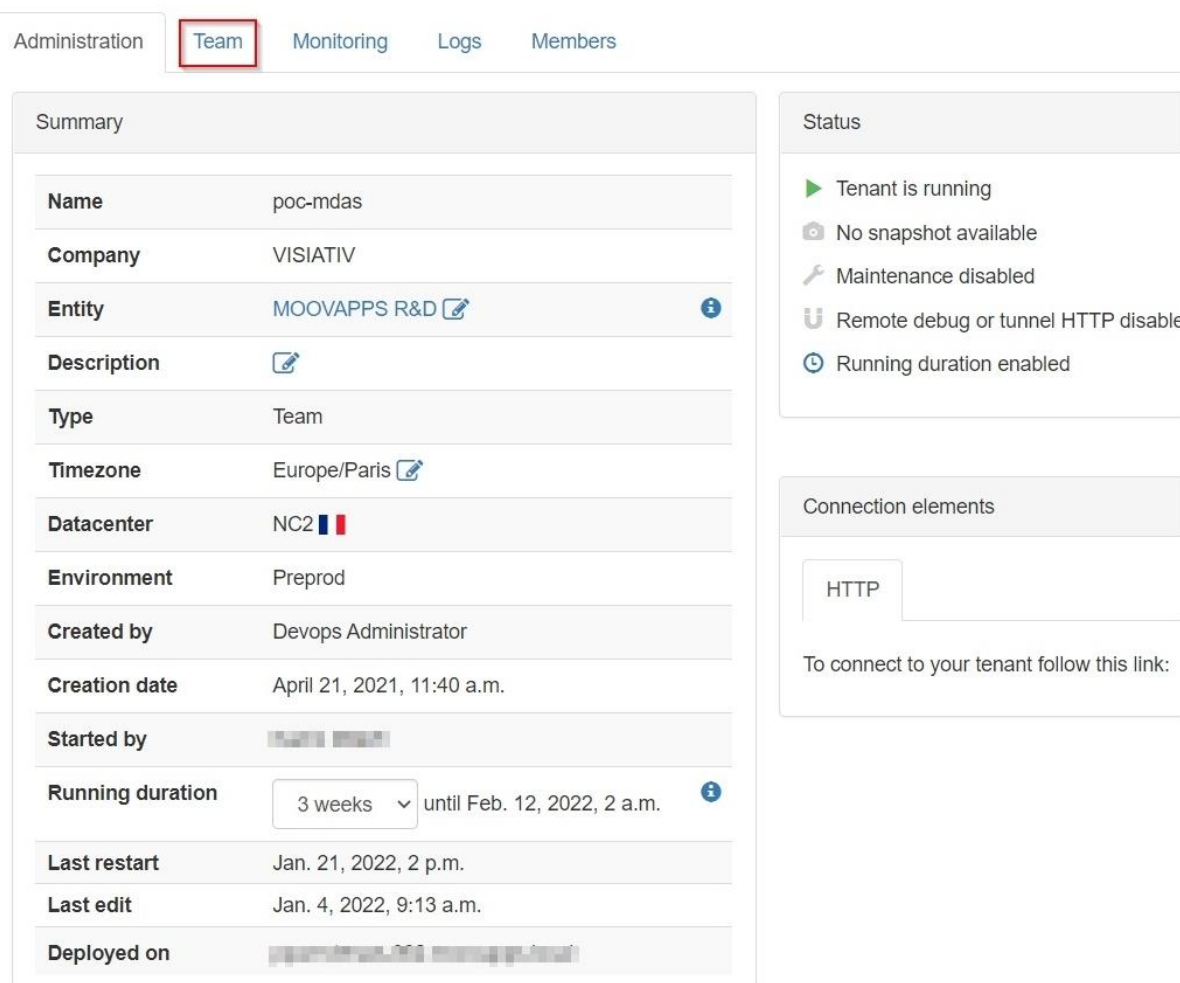
<https://sso.doc.moovapps.com/fr/cases/document/>

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**



The screenshot shows the 'Team' configuration page in Visiativ Cloud Manager. The 'Team' tab is selected and highlighted with a red box. The page is divided into two main sections: 'Summary' and 'Status'.

Summary Section:

Name	poc-mdas
Company	VISIATIV
Entity	MOOVAPPS R&D
Description	
Type	Team
Timezone	Europe/Paris
Datacenter	NC2
Environment	Preprod
Created by	Devops Administrator
Creation date	April 21, 2021, 11:40 a.m.
Started by	
Running duration	3 weeks until Feb. 12, 2022, 2 a.m.
Last restart	Jan. 21, 2022, 2 p.m.
Last edit	Jan. 4, 2022, 9:13 a.m.
Deployed on	

Status Section:

- Tenant is running
- No snapshot available
- Maintenance disabled
- Remote debug or tunnel HTTP disable
- Running duration enabled

Connection elements Section:

HTTP

To connect to your tenant follow this link:

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

Administration Team Monitoring Logs Members

Moovapps Team Specific Deployment ⓘ

Redeploy

Access to configurator ⓘ

Login: api-user

Password:

Configurator:

Links to other products ⓘ

Name	Product	URL	Config	Delete
document-web	Generic SSO		<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>
md-clientweb	Generic SSO		<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>
MD-Local-Test	Generic SSO		<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>
SRVDEV	Generic SSO		<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>
workplace	Workplace	https://poc-mdas.████████████████████.com/moovapps	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>

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 :

Link information



Product : Generic SSO

OIDC

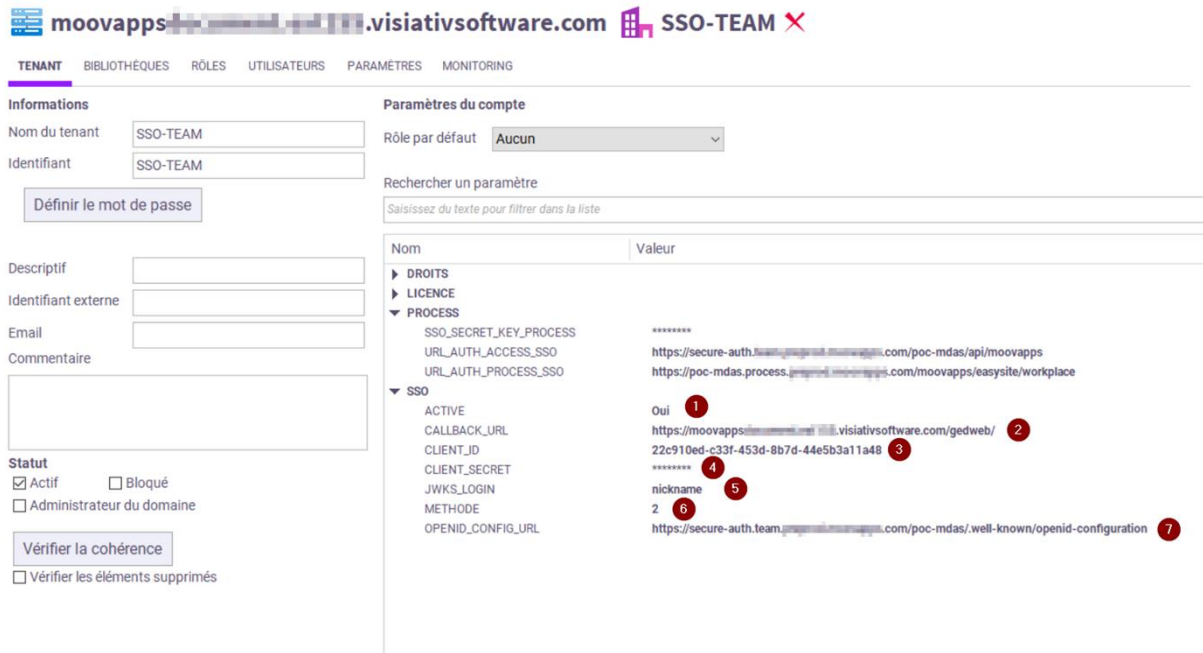
```
Name : poc-sso-oidc
Type : SSO (OIDC)
Grant Type : Authorization code
Auth URL : https://secure-auth.team.poc.poc.moovapps.com/poc-mdas/auth/oauth2/authorize
Access Token URL : https://secure-auth.team.poc.poc.moovapps.com/poc-mdas/auth/oauth2/token
Client ID : 2cad1a5a-9911-49a3-b51c-db8dbb3bac80
Client Secret : 4ChXlFYg[REDACTED] FjNfqj2WYw
Redirect URIs :
  - https://moovapps[REDACTED].visiativsoftware.com/gedweb/sso_login_callback

Post logout redirect URIs :
  - https://moovapps[REDACTED].visiativsoftware.com/gedweb/sso_logout_callback

Front channel logout URIs :
```

Close

Paramétrer le serveur Visiativ Document



Nom	Valeur
▶ DROITS	
▶ LICENCE	
▼ PROCESS	
SSO_SECRET_KEY_PROCESS	*****
URL_AUTH_ACCESS_SSO	https://secure-auth.visiativsoftware.com/poc-mdas/api/moovapps
URL_AUTH_PROCESS_SSO	https://poc-mdas.process.visiativsoftware.com/moovapps/easysite/workplace
▼ SSO	
ACTIVE	Oui 1
CALLBACK_URL	https://moovapps.visiativsoftware.com/gedweb/ 2
CLIENT_ID	22c910ed-c33f-453d-8b7d-44e5b3a11a48 3
CLIENT_SECRET	***** 4
JWKS_LOGIN	nickname 5
METHODE	2 6
OPENID_CONFIG_URL	https://secure-auth.team.visiativsoftware.com/poc-mdas/well-known/openid-configuration 7

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 ».

moovapps [redacted].visiativsoftware.com SSO-TEAM ✕

TENANT BIBLIOTHÈQUES RÔLES UTILISATEURS PARAMÈTRES MONITORING

Informations

Nom du tenant: SSO-TEAM
 Identifiant: SSO-TEAM
 [Définir le mot de passe]

Descriptif: []
 Identifiant externe: []
 Email: []
 Commentaire: []

Statut

Actif Bloqué
 Administrateur du domaine

Paramètres du compte

Rôle par défaut: Aucun

Rechercher un paramètre: [Saisissez du texte pour filtrer dans la liste]

Nom	Valeur
▶ DROITS	
▶ LICENCE	
▼ PROCESS	
SSO_SECRET_KEY_PROCESS	*****
URL_AUTH_ACCESS_SSO	https://secure-auth.[redacted].com/poc-mdas/api/moovapps 1
URL_AUTH_PROCESS_SSO	https://poc-mdas.process.[redacted].com/moovapps/easysite/workplace 2
▶ SSO	

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 la 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
```

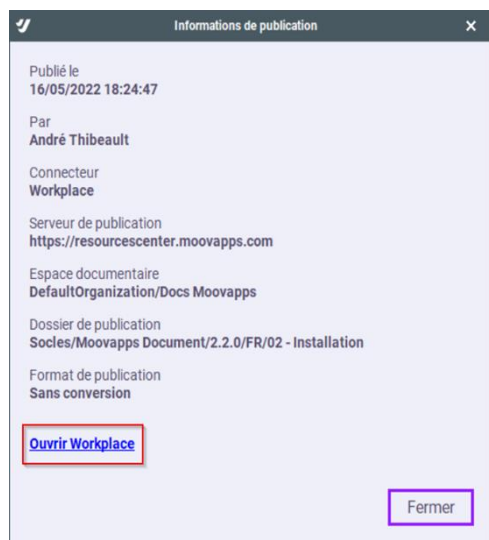
<nom_du_tenant> représente le nom du tenant

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`