



Guide de paramétrage

CONSOLE D'ADMINISTRATION

Version 4.6

Numéro de révision : 7

Date de publication : juin 2023

Auteur : Équipe documentation

Copyright © 2006-2023 Akuiteo S.A.S. Tous droits réservés.

Toute reproduction ou représentation, intégrale ou partielle, faite sans le consentement de l'auteur, serait illicite et constituerait une contrefaçon. La loi n'autorise que les copies ou reproductions réservées à l'usage privé du copiste et non destinées à l'utilisation collective, d'une part, et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration.

L'appellation et les logos Akuiteo sont des marques déposées de la société Akuiteo S.A.S. Toute utilisation de ces marques sans autorisation de la société Akuiteo S.A.S. est interdite.

Visitez : <http://www.akuiteo.com> et <http://www.akuiteo.com/blog/>

Table des Matières

1	Préface	4
1.1	Révisions	4
1.2	Support	4
2	Accéder à la Console d'administration	5
2.1	Se connecter à la console	5
2.2	Changer la langue	5
2.3	Changer le thème	5
2.4	Se déconnecter de la console	6
3	Configurer Akuiteo depuis la Console d'administration	7
3.1	Configurer l'OCR	7
3.2	Configurer la connexion à l'API SIRENE	8
3.2.1	Ajouter le certificat Certigna au serveur Tomcat	8
3.2.2	Paramétrer la Console d'administration	9
3.3	Configurer la connexion au serveur Exchange	9
3.4	Configurer la dématérialisation des factures	12
3.5	Configurer le proxy pour se connecter à Chorus	13
3.6	Configurer la signature électronique	14
3.7	Configurer Akuiteo Connect	15
4	Configurer les méthodes d'authentification	17
4.1	Configurer l'authentification LDAP	17
4.1.1	Prérequis	17
4.1.2	Configurer la Console d'administration	17
4.2	Configurer l'authentification Azure AD	19
4.2.1	Accéder au portail Azure	19
4.2.2	Déclarer Akuiteo comme application de l'annuaire Azure AD	19
4.2.3	Créer un "secret client" pour identifier le serveur Akuiteo	21
4.2.4	Autoriser l'application Akuiteo	21
4.2.5	Configurer la Console d'administration	22
4.3	Configurer l'authentification SAML	23
4.3.1	Prérequis	23
4.3.2	Préparer la configuration	23
4.3.3	Créer une application SAML	26
4.3.4	Configurer la Console d'administration	27
4.4	Configurer l'authentification Oauth2	28

1 Préface

1.1 RÉVISIONS

Révision 7	Publiée en juin 2023 <ul style="list-style-type: none">• Ajout des paramètres liés à l'authentification OAUTH dans Configurer la connexion au serveur Exchange (p. 9).• Ajout du sous-chapitre Configurer le proxy pour se connecter à Chorus (p. 13).
Révision 6	Publiée en août 2022 <ul style="list-style-type: none">• Mise à jour du sous-chapitre Ajouter le certificat Certigna au serveur Tomcat (p. 8).
Révision 5	Publiée en mai 2022 <ul style="list-style-type: none">• Possibilité de récupérer un mot de passe oublié (voir Se connecter à la console (p. 5)).
Révision 4	Publiée en avril 2022 <ul style="list-style-type: none">• Ajout du chapitre Configurer les méthodes d'authentification (p. 17).
Révision 3	Publiée en février 2022 <ul style="list-style-type: none">• Prise en compte de l'API Sirene en création de fournisseurs (voir Configurer la connexion à l'API SIRENE (p. 8)).
Révision 2	Publiée en janvier 2022 <ul style="list-style-type: none">• Précision des API Sirene et Métadonnées pour Configurer la connexion à l'API SIRENE (p. 8).
Révision 1	Publiée en novembre 2021 <ul style="list-style-type: none">• Ajout du chapitre Accéder à la Console d'administration (p. 5).• Mise à jour du sous-chapitre Configurer la dématérialisation des factures (p. 12) pour le multi-société.• Ajout du sous-chapitre Configurer Akuiteo Connect (p. 15).

1.2 SUPPORT

Akuiteo S.A.S. attache une grande importance à votre satisfaction.

Pour nous faire part de vos retours ou contacter le support, visitez la page :

<https://www.akuiteo.fr/akuiteo.clients/>

2 Accéder à la Console d'administration

2.1 SE CONNECTER À LA CONSOLE

- 1 Dans un navigateur web, entrez l'adresse de type `https://nomdomaine/nomserveur/apps/admin/` ou ouvrez le Launcher pour accéder à la Console d'administration.

Exemple

`https://www.akuiteo.fr/akuiteo/apps/admin/`

Note

Pour accéder à la Console d'administration depuis le Launcher, le lien vers l'application doit avoir été initialisé depuis la console. Pour plus d'informations, voir le *Guide Général - Launcher*.

- 2 Dans la fenêtre de connexion, renseignez l'identifiant dans le champ **Utilisateur** et renseignez le **Mot de passe**.

- 3 Cliquez sur **Connexion**.

↳ La page d'accueil de la Console d'administration s'ouvre.

Astuce

Vous avez oublié votre mot de passe ? Dans la fenêtre de connexion, renseignez l'identifiant dans le champ **Utilisateur** et cliquez sur **Mot de passe oublié ?**, puis confirmez la réinitialisation du mot de passe. Un mail vous sera envoyé afin de modifier vos identifiants de connexion.

2.2 CHANGER LA LANGUE

Pour changer la langue de l'interface, cliquez sur l'image de l'utilisateur connecté dans l'en-tête puis cliquez sur le drapeau représentant la langue souhaitée. L'interface est mise à jour automatiquement dans la langue sélectionnée.

2.3 CHANGER LE THÈME

Pour changer le thème visuel de l'interface, cliquez sur l'image de l'utilisateur connecté dans l'en-tête puis cliquez sur le thème Dark ou Light. L'interface est mise à jour automatiquement avec le thème sélectionné.

2.4 SE DÉCONNECTER DE LA CONSOLE

Pour se déconnecter de la console, cliquez sur l'image de l'utilisateur connecté dans l'en-tête puis cliquez sur **Déconnexion**.

3 Configurer Akuiteo depuis la Console d'administration

3.1 CONFIGURER L'OCR

L'OCR (Optical Character Recognition), ou reconnaissance optique de caractères en français, est une technologie qui permet de convertir différents types de documents tels que les documents papiers numérisés, les fichiers PDF ou les photos numériques en fichiers modifiables et interrogeables. Un logiciel d'OCR sera ainsi capable de reconnaître les lettres contenues dans les images et de reconstituer des mots ou des phrases entières.

Akuiteo intègre un système d'OCR pour simplifier la saisie des dépenses dans une note de frais depuis le Portail Collaborateur et l'application Akuiteo Mobile. Lorsqu'un justificatif est pris en photo, les caractères sont reconnus automatiquement et sont ainsi ajoutés dans les champs concernés de la dépense.

L'OCR est configuré dans la Console d'Administration, depuis le menu **Configuration > OCR**.

- 1 Dans l'écran **Configuration OCR**, sélectionnez **OCR_MINDEE** dans la liste déroulante du champ **provider**.
- 2 Renseignez les champs suivants pour configurer l'OCR :

Champ	Description
OCR Actif	Cochez la case pour activer l'OCR de façon globale.
Mindee Actif	Cochez la case pour activer l'OCR Mindee sur le Portail Collaborateur et l'application Akuiteo Mobile.
Url de connexion	Renseignez l'URL de connexion au web service, fourni par Akuiteo.
Token Mindee	Renseignez le token fourni par Akuiteo pour accéder au web service.
Utilisateur Akuiteo	Renseignez le login Akuiteo permettant de se connecter au web service. Cet utilisateur est utilisé pour différencier les dépenses saisies en utilisant l'OCR des dépenses saisies par le collaborateur. Lorsqu'une dépense est saisie grâce à l'OCR, l'utilisateur Akuiteo est renseigné dans l'historique de la dépense.
Mot de passe Akuiteo	Renseignez le mot de passe associé au login Akuiteo.

- 3 Cliquez sur **Enregistrer** pour chaque champ renseigné ou modifié afin de prendre en compte la valeur renseignée.

- 4 Cliquez sur le bouton **Tester** pour tester la connexion à l'interface OCR Mindee à partir des valeurs renseignées.

3.2 CONFIGURER LA CONNEXION À L'API SIRENE

L'interface avec l'API SIRENE permet de remplir automatiquement les champs concernés lors de la création d'un prospect, d'un client ou d'un fournisseur grâce au numéro de SIRET ou de SIREN renseigné. Si le numéro de SIRET ou de SIREN renseigné est reconnu par l'API SIRENE, alors les champs concernés (comme le nom d'appel ou l'adresse) seront renseignés automatiquement.

3.2.1 Ajouter le certificat Certigna au serveur Tomcat

L'environnement d'exécution Java (JRE) dispose d'un fichier de configuration (keystore) qui comprend les certificats racines des différentes autorités de certification reconnues. Lorsqu'une connexion est établie vers un autre système en https, cette liste de certificats permet de valider la connexion sécurisée.

Certaines autorités de certification ne sont pas présentes dans le fichier fourni par défaut avec le JRE et il est donc nécessaire de les ajouter manuellement. Dans le cas de l'API SIRENE, il vous faut ajouter le certificat Certigna pour certifier les connexions.

Note

Pour les clients SaaS, l'ajout du certificat est effectué par Akuiteo.

Identifier l'emplacement du JRE Java

- 1 Connectez-vous au serveur qui héberge l'environnement Akuiteo.
- 2 Lancez le Manager Tomcat de l'environnement ciblé.
- 3 Depuis l'onglet **Java**, notez l'emplacement du JRE utilisé par Tomcat.

Récupérer le certificat Racine de Certigna

- 1 Rendez-vous sur le site de Certigna : <https://www.certigna.com/autorite-crl>.
- 2 Téléchargez le certificat d'autorité Certigna Racine : *certigna.der*.

Importer le certificat dans le keystore du JRE Java

- 1 Lancez l'invite de commande en mode administrateur.
- 2 Lancez la commande suivante :

```
"[EMPLACEMENT_JRE]\bin\keytool.exe" -import -alias "certigna" -keystore "[EMPLACEMENT_JRE]\lib\security\cacerts" -trustcacerts -file "[EMPLACEMENT_CERTIFICAT]\certigna.der" -storepass changeit
```

Dans cette commande, vous devez remplacer :

- **[EMPLACEMENT_JRE]** par l'emplacement du JRE Java utilisé par Tomcat
- **[EMPLACEMENT_CERTIFICAT]** par l'emplacement du certificat *certigna.der* téléchargé.

Exemple

```
"C:\Program Files\Java\jdk1.8.0_22\jre\bin\keytool.exe" -import -alias
"certigna" -keystore "C:\Program Files\Java\jdk1.8.0_
22\jre\lib\security\cacerts" -trustcacerts -file
"C:\Users\XXX\Documents\certigna.der" -storepass changeit
```

- 3 Redémarrez le serveur Tomcat de l'environnement Akuiteo ciblé pour prendre en compte l'ajout du certificat.

3.2.2 Paramétrer la Console d'administration

La connexion à l'API SIRENE est configurée dans la Console d'Administration, depuis le menu **Configuration > API Sirene**.

- 1 Renseignez les champs suivants pour configurer la connexion :

Champ	Description
Utilisation de l'API SIRENE	Cochez la case pour utiliser l'API SIRENE.
Jeton pour l'API SIRENE	<p>Renseignez le jeton généré depuis le site api.insee.fr.</p> <p>Pour récupérer ce jeton :</p> <ol style="list-style-type: none"> 1. En tant qu'administrateur, créez un compte sur le site api.insee.fr. 2. Activez les API Sirene et Métadonnées pour l'application (Akuiteo). 3. Générez un jeton pour cette application, quel que soit le nombre d'API interrogées, et définissez la durée de validité de ce jeton.

- 2 Cliquez sur **Enregistrer** pour chaque champ renseigné ou modifié afin de prendre en compte la valeur renseignée.
- 3 Cliquez sur le bouton **Tester** pour tester la connexion à l'API SIRENE à partir des valeurs renseignées.

3.3 CONFIGURER LA CONNEXION AU SERVEUR EXCHANGE

Les paramètres de connexion au serveur Exchange sont utilisés pour synchroniser les plannings ou les rendez-vous dans Akuiteo avec un agenda Microsoft Outlook.

La connexion au serveur Exchange est configurée dans la Console d'Administration, depuis le menu **Configuration > Exchange**.

- 1 Renseignez les champs suivants pour configurer la connexion au serveur Exchange :

Champ	Description						
Utilisateur délégué	<p>Renseignez le login de l'utilisateur Exchange pour se connecter au serveur.</p> <p>Si vous utilisez Exchange 365, cet utilisateur doit posséder une délégation d'accès total aux autres comptes des collaborateurs.</p>						
Mot de passe associé	Renseignez le mot de passe associé au login de l'utilisateur Exchange.						
URL du service EWS	<p>Renseignez l'URL de connexion au serveur Exchange.</p> <div> <p>Exemple</p> <p>https://outlook.office365.com/EWS/exchange.asmx</p> </div>						
Version du serveur Exchange	Sélectionnez la version du serveur Exchange depuis la liste déroulante.						
Nombre de threads maximum pour les synchronisations	Renseignez le nombre maximum de synchronisations en simultanée.						
Utiliser la librairie optimisée pour Office 365	Si vous utilisez Exchange 365, cochez cette case afin d'utiliser la librairie optimisée pour Office 365.						
Utiliser l'impersonation	<p>Si vous utilisez Exchange 365, cochez cette case. Office 365 impose des limites sur le nombre d'appel de web services pour un utilisateur donné. L'impersonation permet d'affecter un rôle à un utilisateur Exchange et de contourner cette limitation.</p> <p>Pour utiliser l'impersonation, vous devez au préalable :</p> <p>Supprimer toutes les délégations de compte de l'utilisateur technique Exchange</p> <ol style="list-style-type: none"> 1. Téléchargez et installez PowerShell. 2. Depuis PowerShell, exécutez les commandes suivantes : <table> <tr> <td> <pre>\$Session = New-PSSession - ConfigurationName Microsoft.Exchange - ConnectionUri https://outlook.office365.com/powershell- liveid/ -Credential \$UserCredential - Authentication Basic -AllowRedirection</pre> </td><td>Cette commande permet d'établir une connexion au serveur Exchange. Le login et mot de passe de l'administrateur sont requis.</td></tr> <tr> <td> <pre>Import-PSSession \$Session</pre> </td><td>Cette commande permet de récupérer des commandes nécessaires pour supprimer les délégations.</td></tr> <tr> <td> <pre>foreach (\$mailbox in Get-Mailbox) { Remove-MailboxPermission \$mailbox.PrimarySmtpAddress -user user@domain -Accessright FullAccess -</pre> </td><td>Remplacez user@domain par le login de l'utilisateur technique actuel Akuiteo</td></tr> </table>	<pre>\$Session = New-PSSession - ConfigurationName Microsoft.Exchange - ConnectionUri https://outlook.office365.com/powershell- liveid/ -Credential \$UserCredential - Authentication Basic -AllowRedirection</pre>	Cette commande permet d'établir une connexion au serveur Exchange. Le login et mot de passe de l'administrateur sont requis.	<pre>Import-PSSession \$Session</pre>	Cette commande permet de récupérer des commandes nécessaires pour supprimer les délégations.	<pre>foreach (\$mailbox in Get-Mailbox) { Remove-MailboxPermission \$mailbox.PrimarySmtpAddress -user user@domain -Accessright FullAccess -</pre>	Remplacez user@domain par le login de l'utilisateur technique actuel Akuiteo
<pre>\$Session = New-PSSession - ConfigurationName Microsoft.Exchange - ConnectionUri https://outlook.office365.com/powershell- liveid/ -Credential \$UserCredential - Authentication Basic -AllowRedirection</pre>	Cette commande permet d'établir une connexion au serveur Exchange. Le login et mot de passe de l'administrateur sont requis.						
<pre>Import-PSSession \$Session</pre>	Cette commande permet de récupérer des commandes nécessaires pour supprimer les délégations.						
<pre>foreach (\$mailbox in Get-Mailbox) { Remove-MailboxPermission \$mailbox.PrimarySmtpAddress -user user@domain -Accessright FullAccess -</pre>	Remplacez user@domain par le login de l'utilisateur technique actuel Akuiteo						

Champ	Description
	<div> <div>Confirm: \$false}</div> <div> <p>qui possède le droit de délégation.</p> <p>Cette commande permet de supprimer le rôle de délégation pour tous les utilisateurs.</p> </div> </div> <p>Ajouter le droit d'impersonation à l'utilisateur technique Exchange</p> <ol style="list-style-type: none"> 1. Connectez-vous à la console d'administration Exchange depuis le portail Office 365. 2. Allez dans le menu Autorisations > Rôles d'administrateur. 3. Créez un nouveau rôle en renseignant les éléments suivants : <ul style="list-style-type: none"> • Nom : Application Impersonation • Rôles : Ajoutez les rôles ApplicationImpersonation, Legal Hold et Mailbox Search • Membres : Ajoutez l'utilisateur technique actuel Akuiteo
Utilisateur à tester	Renseignez une adresse mail existante pour s'assurer qu'Akuiteo peut accéder au compte correspondant en utilisant l'impersonation.
Utiliser une authentification OAUTH (Exchange 365 seulement)	<p>Activez ou désactivez l'authentification OAUTH pour la connexion à Exchange.</p> <p>Cette case doit être cochée si Exchange 365 est utilisé par Akuiteo dans votre organisation. Dans les autres cas, cette case doit être décochée.</p>
Tenant ID	<p>Ce champ doit être renseigné si Utiliser une authentification OAUTH (Exchange 365 seulement) est coché.</p> <p>Renseignez l'identifiant de locataire fourni par Microsoft pour l'authentification OAUTH.</p>
Client ID	<p>Ce champ doit être renseigné si Utiliser une authentification OAUTH (Exchange 365 seulement) est coché.</p> <p>Renseignez l'identifiant du client pour l'authentification OAUTH.</p>
Client Secret	<p>Ce champ doit être renseigné si Utiliser une authentification OAUTH (Exchange 365 seulement) est coché.</p> <p>Renseignez le secret du client pour l'authentification OAUTH.</p>

- 2 Cliquez sur **Enregistrer** pour chaque champ renseigné ou modifié afin de prendre en compte la valeur renseignée.
- 3 Cliquez sur le bouton **Tester** pour tester la connexion à l'interface Exchange à partir des valeurs renseignées.

3.4 CONFIGURER LA DÉMATÉRIALISATION DES FACTURES

Les paramètres de configuration pour l'interface avec CHORUS PRO permettent de mettre en place la transmission automatique vers le portail CHORUS PRO des factures dématérialisées générées par Akuiteo. Il est ainsi possible de générer et de transmettre automatiquement les factures dématérialisées depuis l'Application Desktop, sans avoir besoin d'utiliser un outil externe ou de transmettre manuellement les factures.

La transmission automatique des factures dématérialisées est configurée dans la Console d'Administration, depuis le menu **Configuration > Dématérialisation**.

Notes

Pour les clients SaaS, le paramétrage de la Console d'administration est effectué par Akuiteo.

Référence

Les identifiants de connexion à CHORUS PRO doivent être renseignés depuis le paramétrage de l'Application Desktop pour permettre d'utiliser différents comptes CHORUS PRO en fonction de chaque société. Pour plus d'informations, voir le *Guide Paramétrage - Dématérialisation Chorus*.

1 Renseignez les champs suivants pour configurer la connexion à CHORUS PRO :

Champ	Description
Chorus Actif	Cochez la case pour activer la connexion à CHORUS PRO.
URL Authentification Chorus	Renseignez l'URL d'authentification à CHORUS PRO : <ul style="list-style-type: none">• https://sandbox-oauth.aife.economie.gouv.fr/api/oauth/token pour les environnements de test,• https://oauth.aife.economie.gouv.fr/api/oauth/token pour les environnements de production.
Url	Renseignez l'URL de connexion à CHORUS PRO : <ul style="list-style-type: none">• https://sandbox-api.aife.economie.gouv.fr/ pour les environnements de test,• https://api.aife.economie.gouv.fr/ pour les environnements de production.

2 Renseignez les champs suivants pour configurer l'interface entre Akuiteo et CHORUS PRO :

Champ	Description
Utilisateur Akuiteo	Renseignez le login de l'utilisateur technique Akuiteo.
Mot de passe de l'utilisateur Akuiteo	Renseignez le mot de passe associé au login Akuiteo.
Code de la société de connexion de	Renseignez le code de la société de connexion.

Champ	Description
l'utilisateur Akuiteo	
Nombre d'essais successifs en cas d'erreur	<p>Le nombre d'essais successifs permet de renseigner, en cas d'erreur lors de la transmission des factures dématérialisées, le nombre de fois où Akuiteo peut réessayer la transmission.</p> <p>Par défaut, Akuiteo effectue 3 essais successifs en cas d'erreur.</p>
Délai en seconde entre chaque essai successif	<p>Le délai entre chaque essai successif permet de renseigner, en secondes, le délai d'attente avant de relancer un essai de transmission en cas d'erreur.</p> <p>Par défaut, Akuiteo attend 10 secondes entre chaque essai successif.</p>
Nombre d'appels maximum à Chorus par seconde	<p>Renseignez le nombre maximum d'appels en simultanée par seconde à CHORUS PRO.</p> <p>Par défaut, on autorise au maximum 20 appels par seconde. Pour un environnement de test, le nombre doit être fixé à 1 appel maximum par seconde.</p>

Note

Le portail CHORUS PRO possède des quotas pour la transmission des factures dématérialisées :

- Sur l'espace de test : 5 requêtes par seconde avec 50 000 requêtes par jour maximum
- Sur l'espace de production : 20 requêtes par seconde avec 1 million de requêtes par jour maximum

Si ces quotas sont atteints, la transmission des factures est bloquée. Adaptez les valeurs dans les champs **Nombre d'essais successifs en cas d'erreur** et **Délai en seconde entre chaque essai successif** si vous constatez régulièrement des erreurs lors du dépôt des factures.

- 3 Cliquez sur **Enregistrer** pour chaque champ renseigné ou modifié afin de prendre en compte la valeur renseignée.

3.5 CONFIGURER LE PROXY POUR SE CONNECTER À CHORUS

Un proxy est un serveur qui agit comme une passerelle entre un ordinateur et les serveurs externes.

Si votre organisation a mis en place un proxy, il est possible de le renseigner dans la Console d'administration afin qu'Akuiteo passe par le proxy pour se connecter à Chorus.

Le proxy est renseigné dans la Console d'administration, depuis **Configuration > Configuration du proxy**.

Pour renseigner le proxy :

- 1 Sur la page **Configuration PROXY**, renseignez les informations suivantes :

Champ	Description
Proxy URL	Renseignez l'adresse IP et le port du proxy. Ex : http://10.69.20.73:9999
Proxy UserName	Renseignez le nom d'utilisateur pour se connecter au proxy.
Proxy Password	Renseignez le mot de passe pour se connecter au proxy.

2 Pour chaque information renseignée, cliquez sur **Enregistrer**.

↳ Le proxy est configuré.

3.6 CONFIGURER LA SIGNATURE ÉLECTRONIQUE

Les paramètres de configuration des APIs Universign permettent de mettre en place la signature électronique pour les devis et les bons de livraison client. L'interface avec ces APIs permet donc d'envoyer les devis et bons de livraison à signer électroniquement aux clients directement depuis l'Application Desktop, sans avoir besoin de passer par une interface supplémentaire.

La signature électronique est configurée dans la Console d'Administration, depuis le menu **Configuration > Signature électronique**.

1 Renseignez les champs suivants pour configurer la signature électronique :

Champ	Description
Activer la signature électronique	Cochez la case pour activer la signature électronique.
URL Universign	Renseignez l'URL fourni par Akuteo pour se connecter aux APIs Universign.
Utilisateur universign	Renseignez le login de l'utilisateur Universign, fourni par Akuteo.
Mot de passe universign	Renseignez le mot de passe associé au login Universign, fourni par Akuteo.
Utilisateur Akuteo	Renseignez le login de l'utilisateur technique Akuteo utilisé pour se connecter aux APIs.
Mot de passe Akuteo	Renseignez le mot de passe associé au login de l'utilisateur technique Akuteo.
Intervalle de récupération des signatures	<p>Une tâche planifiée est exécutée en tâche de fond afin de chercher l'état des signataires (si les destinataires pour la signature électronique ont signé ou non) et, une fois toutes les signatures effectuées, afin de récupérer les documents signés.</p> <p>L'intervalle de récupération des signatures permet de renseigner, en secondes, l'intervalle d'exécution de cette tâche planifiée.</p> <p>Par défaut, la tâche s'exécute toutes les 21600 secondes, soit 6 heures.</p>

Champ	Description
	<p>Note</p> <p>Il est déconseillé de renseigner un intervalle trop bas pour ne pas surcharger les appels.</p>
Délai de démarrage	<p>Le délai de démarrage permet de renseigner, en secondes, le délai pour lancer la première tâche planifiée après le démarrage du serveur Akuiteo.</p> <p>Par défaut, la tâche est exécutée pour la première fois 20 secondes après le démarrage du serveur.</p>

- 2 Cliquez sur **Enregistrer** pour chaque champ renseigné ou modifié afin de prendre en compte la valeur renseignée.
- 3 Cliquez sur le bouton **Tester** pour tester la connexion aux APIs Universign à partir des valeurs renseignées.

3.7 CONFIGURER AKUITEO CONNECT

Les paramètres de configuration Akuiteo Connect permettent de se connecter au connecteur Bridge pour mettre en place la récupération automatique et sécurisée des transactions bancaires dans Akuiteo. L'interface avec Bridge permet ainsi de récupérer les opérations bancaires directement depuis votre banque sans avoir à importer manuellement des fichiers de relevés bancaires.

La connexion à Akuiteo Connect est configurée dans la Console d'Administration, depuis le menu **Configuration > Akuiteo Connect**.

Important

Au préalable, Akuiteo doit paramétrer les identifiants de votre compte Bridge pour vous permettre d'activer et de configurer Akuiteo Connect.

Configurer la connexion à Akuiteo Connect

- 1 Dans la section **Akuiteo Connect**, renseignez les champs suivants pour configurer la connexion :

Champ	Description
Activer Akuiteo Connect	Cochez la case pour activer la connexion à Akuiteo Connect.
Utilisateur Akuiteo	Renseignez le login de l'utilisateur technique Akuiteo. Cet utilisateur sera utilisé pour créer les nouveaux relevés à partir des transactions bancaires récupérées.
Mot de passe Akuiteo	Renseignez le mot de passe associé au login Akuiteo.
Email	Renseignez l'adresse mail à laquelle seront envoyés les logs d'exécution de la tâche planifiée.

Champ	Description
Intervalle de récupération des relevés	<p>Une tâche planifiée est exécutée en tâche de fond pour récupérer les transactions des comptes bancaires connectés. Les transactions sont stockées dans une table intermédiaire en attendant la génération d'un relevé.</p> <p>L'intervalle de récupération des transactions bancaires permet de renseigner, en secondes, l'intervalle d'exécution de cette tâche planifiée.</p> <p>Par défaut, la tâche s'exécute toutes les 21600 secondes.</p> <div> <p>Note</p> <p>Il est déconseillé de renseigner un intervalle trop bas pour ne pas surcharger les appels.</p> </div>
Délai de démarrage (par défaut 20s)	<p>Le délai de démarrage permet de renseigner, en secondes, le délai pour lancer la première tâche planifiée après le démarrage du serveur Akuiteo.</p> <p>Par défaut, la tâche est exécutée pour la première fois 20 secondes après le démarrage du serveur.</p>

- 2 Cliquez sur **Enregistrer** pour chaque champ renseigné ou modifié afin de prendre en compte la valeur renseignée.
- 3 Cliquez sur le bouton **Tester** pour tester la connexion à Akuiteo Connect à partir des valeurs renseignées.

Ajouter un utilisateur Bridge


Note


Vous pouvez seulement ajouter un utilisateur Bridge. En effet, un client d'Akuiteo est associé à un seul compte/utilisateur Bridge.

L'utilisateur du compte créé depuis Bridge doit être ajouté dans la Console d'administration pour lier les comptes bancaires associés à cet utilisateur Bridge dans Akuiteo. Cet utilisateur Bridge est lié nominativement aux comptes bancaires de toutes les sociétés mais l'accès aux comptes bancaires reste soumis à l'authentification du détenteur de chaque compte.

- 1 Dans la section **Utilisateur Bridge**, cliquez sur **Créer un nouvel utilisateur Bridge**.
- 2 Dans la fenêtre, renseignez les **Nom**, **Email** et **Mot de passe** utilisés pour créer le compte Bridge.
- 3 Cliquez sur **Créer**.

↳ L'utilisateur Bridge est ajouté à la Console d'administration.

Pour modifier les informations de l'utilisateur, cliquez sur , modifiez les informations souhaitées puis cliquez sur **Mettre à jour**.

Pour supprimer l'utilisateur, supprimez toutes ses banques associées puis cliquez sur  et confirmez la suppression.

4 Configurer les méthodes d'authentification

Akuiteo permet de gérer l'authentification des utilisateurs de plusieurs façons :

- L'authentification propre à Akuiteo, qui n'est pas évoquée dans ce chapitre. Les utilisateurs et leurs mots de passe associés sont paramétrés dans l'Application Desktop et sont stockés en base de données.
- L'authentification LDAP, où les utilisateurs sont déclarés dans un annuaire LDAP (Active Directory par exemple). Voir [Configurer l'authentification LDAP \(p. 17\)](#).
- L'authentification Azure Active Directory, un service fourni par Microsoft pour tous les clients Office 365. Voir [Configurer l'authentification Azure AD \(p. 19\)](#).
- L'authentification SAML (Security Assertion Markup Language), un standard ouvert qui permet à diverses applications de s'authentifier de manière unique auprès d'un portail d'identification. SAML est standardisé et permet ainsi d'avoir recours au produit utilisé par votre entreprise (Azure AD ou Okta par exemple). Voir [Configurer l'authentification SAML \(p. 23\)](#).
- L'authentification OAuth2, utilisée uniquement pour faire appel aux APIs Akuiteo. Voir [Configurer l'authentification OAuth2 \(p. 28\)](#).

4.1 CONFIGURER L'AUTHENTIFICATION LDAP

4.1.1 Prérequis

Pour mettre en place un lien vers un annuaire LDAP, vérifiez les points suivants :

- Si un pare-feu est présent entre le serveur Akuiteo et l'annuaire, celui-ci doit être configuré pour laisser passer les communications sur le port adéquat (389 par exemple).
- Un compte dit "technique" doit être créé avec les caractéristiques suivantes :
 - Le compte peut accéder en lecture à l'ensemble de l'annuaire.
 - Le compte peut lire tous les attributs d'un élément de l'annuaire.
 - Le compte n'est pas verrouillé.
 - Le mot de passe ne peut et ne doit pas être changé, et n'expire jamais.
- Les utilisateurs déclarés dans Akuiteo doivent avoir pour identifiant celui utilisé dans le LDAP.

Exemple

Si l'utilisateur Jean Dupont est déclaré dans l'annuaire en tant que *JDT*, l'identifiant de cet utilisateur dans Akuiteo doit également être *JDT*.

4.1.2 Configurer la Console d'administration


Les coordonnées pour accéder à un annuaire LDAP sont définies dans la Console d'administration, depuis le menu **Sécurité > LDAP**.


- 1 Depuis l'écran **LDAP**, cliquez sur le bouton **Créer une nouvelle configuration** en haut à droite de l'écran.
- 2 Dans la fenêtre de configuration, renseignez les champs suivants :

Champ	Description
Code	Attribuez un code à l'annuaire pour l'identifier. Ce code doit être unique.
Login	<p>Renseignez l'identifiant complet du compte technique, par exemple <i>CN=LDAPBrowser,OU=Technique,OU=Republique,DC=akuiteo,DC=lan</i>.</p> <div> <p>Astuce</p> <p>Si vous utilisez Active Directory, cet identifiant est indiqué dans les propriétés de l'utilisateur dit "technique" > onglet Éditeur d'attributs > attribut distinguishedName.</p> </div>
Password	Renseignez le mot de passe associé au compte technique.
Dn Base	<p>Renseignez le chemin qui pointe vers le début de l'arborescence, par exemple <i>OU=Republique,DC=akuiteo,DC=lan</i>.</p> <div> <p>Astuce</p> <p>Si vous utilisez Active Directory, cet identifiant est indiqué dans les propriétés à la racine de l'arborescence des utilisateurs > onglet Éditeur d'attributs > attribut dnBase.</p> </div>
URL	<p>Renseignez le nom ou l'adresse IP du serveur LDAP, avec le port de communication pour les accès LDAP (389 par défaut). L'adresse est de type : <i>ldap://serveur:389</i>.</p> <p>Il est possible de renseigner autant d'URLs que nécessaire, par exemple en cas de panne d'un serveur. Dans ce cas, l'URL 1 est utilisée en priorité. Si cette URL ne fonctionne pas, c'est l'URL 2 qui est utilisée, et ainsi de suite. Cette bascule se fait automatiquement lorsque l'annuaire courant ne répond plus, sans avoir besoin de redémarrer le serveur Akuiteo.</p>
Par défaut	<p>Si vous avez plusieurs serveurs configurés, cochez cette case pour préciser le serveur à utiliser.</p> <p>Si vous n'avez qu'un seul serveur configuré, vous devez cocher cette case.</p>
Authentification	<p>Cochez cette case pour activer l'authentification avec l'annuaire LDAP.</p> <p>Si cette case n'est pas cochée, l'authentification sera fondée sur une autre méthode d'authentification (si activée) ou sur la base de données.</p>

- 3 Cliquez sur **Tester puis enregistrer** pour tester la connexion à l'annuaire LDAP à partir des valeurs renseignées.

↳ Si la connexion est établie, l'annuaire est ajouté dans la Console d'administration. Si la connexion ne peut pas être établie, un message d'erreur est affiché.

Pour modifier les informations d'un annuaire, cliquez sur  pour l'annuaire concerné, modifiez les informations souhaitées puis cliquez sur **Tester puis enregistrer**.

Pour supprimer un annuaire, cliquez sur  pour l'annuaire concerné et confirmez la suppression.

4.2 CONFIGURER L'AUTHENTIFICATION AZURE AD

Important

Akuiteo n'est pas compatible avec l'utilisation d'une authentification multifacteur (MFA) coté Azure ou Office 365.

Note

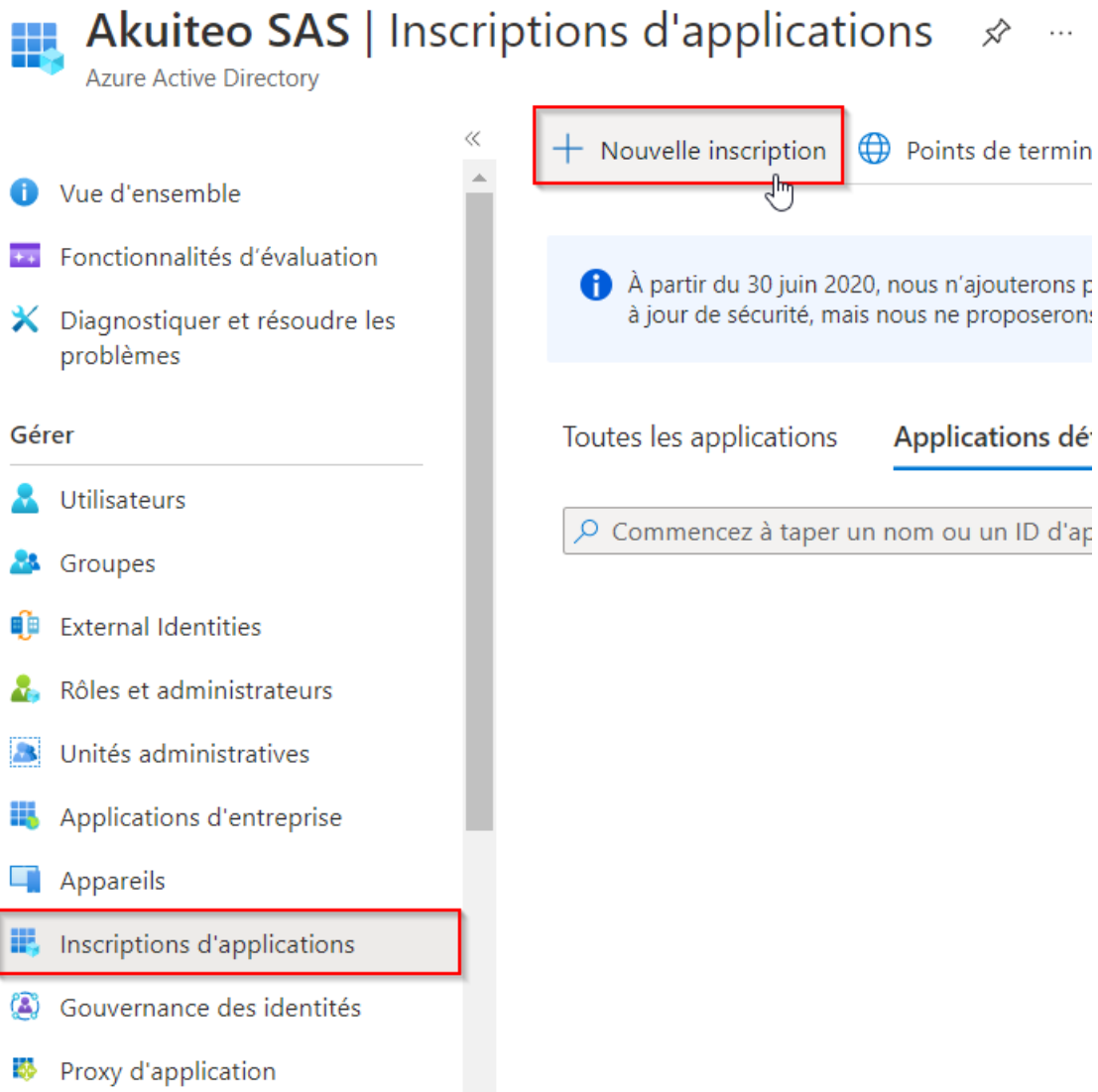
L'authentification entre Akuiteo et Azure AD utilise une adresse mail comme identifiant. Cette adresse doit donc être paramétrée correctement dans Akuiteo pour que l'utilisateur puisse se connecter.

4.2.1 Accéder au portail Azure

- 1 Dans un navigateur web, entrez l'adresse <https://portal.azure.com/> et connectez-vous en tant qu'administrateur.
- 2 Sur la page d'accueil, cliquez sur le bouton **Voir** dans la section **Gérer Azure Active Directory**.

4.2.2 Déclarer Akuiteo comme application de l'annuaire Azure AD

- 1 Cliquez sur **Inscriptions d'applications** dans le menu de gauche, puis cliquez sur **Nouvelle inscription**.



- 2 Renseignez le **Nom** de cette nouvelle inscription (par exemple *Akuiteo*) et laissez l'option **Comptes dans cet annuaire d'organisation uniquement (XXX uniquement - Locataire unique)** cochée. Cliquez ensuite sur **S'inscrire**.

↳ La page de l'application est affichée avec les informations suivantes :

- **ID d'application (client)** : correspond au Client ID dans Akuiteo
- **ID de l'annuaire (locataire)** : correspond au Tenant ID dans Akuiteo
- **ID de l'objet** : correspond à l'Application ID dans Akuiteo

- 3 Passez la souris sur chacun de ces champs puis cliquez sur l'icône permettant de copier l'information dans le presse-papiers. Conservez ces informations dans un document à part.

^ Bases

Nom d'affichage : [Akuiteo](#)

ID d'application (client) : 94946e61-e7eb-4837-8876-c07a454bc767

ID de l'objet : 47abfc6b-934c-43a9-8503-3ecf6e25bc58

ID de l'annuaire (locataire) : fe36d35c-1016-45f5-ae00-5c283df33f73

Types de comptes pris en... : [Mon organisation uniquement](#)

Copier dans le Presse-papiers

4.2.3 Créer un "secret client" pour identifier le serveur Akuiteo

- 1 Cliquez sur **Certificats & secrets** dans le menu de gauche, puis cliquez sur **Nouveau secret client**.

Authentification

Certificats & secrets

Configuration du jeton

API autorisées

Exposer une API

Rôles d'application

Propriétaires

Certificats (0) **Secrets client (0)** Informations d'identité

Chaîne secrète que l'application utilise pour prouver son identité

+ Nouveau secret client

Description	Date d'expiration
Aucun secret client n'a été créé pour cette application.	

- 2 Renseignez une **Description** (par exemple *Secret Akuiteo*) et sélectionnez la **Date d'expiration** de la clé en fonction de votre politique de sécurité. Cliquez ensuite sur **Ajouter**.

Important

Une fois la date d'expiration passée, vous devrez créer un nouveau "secret client".

- 3 Passez la souris sur la ligne de ce "secret client" puis cliquez sur le bouton permettant de copier l'information dans le presse-papiers. Conservez cette information dans un document à part.

4.2.4 Autoriser l'application Akuiteo

Depuis le menu **API autorisées**, cliquez sur l'API **Microsoft Graph** et assurez-vous que l'application Akuiteo a un statut **Accordé pour** Si ce n'est pas le cas, cliquez sur **Accorder un consentement d'administrateur pour XXX**.

- Authentification
- Certificats & secrets
- Configuration du jeton
- API autorisées**
- Exposer une API
- Rôles d'application
- Propriétaires
- Rôles et administrateurs
- Manifeste

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

+ Ajouter une autorisation ✓ Accorder un consentement d'administrateur pour Akuiteo SAS

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
▼ Microsoft Graph (1)				
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	✓ Accordé pour Akuiteo S...

Pour afficher et gérer les autorisations et le consentement de l'utilisateur, essayez [Applications d'entreprise](#).

Note

Si cette autorisation n'est pas donnée, chaque utilisateur devra d'abord donner son consentement depuis le portail Azure afin d'être autorisé à se connecter à Akuiteo.

4.2.5 Configurer la Console d'administration

Les annuaires Azure AD sont définis dans la Console d'administration, depuis le menu **Sécurité > Azure AD**.

- Depuis l'écran **Azure AD**, cliquez sur le bouton **Créer une nouvelle configuration** en haut à droite de l'écran.
- Dans la fenêtre de configuration, renseignez les champs suivants :

Champ	Description
Code	Attribuez un code à l'annuaire pour l'identifier. Ce code doit être unique.
Tenant Id	Renseignez la valeur du champ ID de l'annuaire (locataire) (dans le portail Azure).
Client Id	Renseignez la valeur du champ ID d'application (client) (dans le portail Azure).
Client Secret	Renseignez la valeur du secret client (dans le portail Azure).
Application Id	Renseignez la valeur du champ ID de l'objet (dans le portail Azure).
Authentification ?	<p>Cochez cette case pour activer l'authentification avec Azure AD.</p> <p>Si la case n'est pas cochée, l'authentification sera fondée sur une autre méthode d'authentification (si activée) ou sur la base de données.</p>

- Cliquez sur **Créer**.
 - ↳ L'annuaire est ajouté dans la Console d'administration.
- Redémarrez le serveur pour que l'annuaire Azure AD soit pris en compte.

Pour modifier les informations d'un annuaire, cliquez sur ✎ pour l'annuaire concerné, modifiez les informations souhaitées puis cliquez sur **Mettre à jour**.

Pour supprimer un annuaire, cliquez sur 🗑 pour l'annuaire concerné et confirmez la suppression.

4.3 CONFIGURER L'AUTHENTIFICATION SAML

La norme SAML (Security Assertion Markup Language) est un standard ouvert qui permet à diverses applications de s'authentifier de manière unique auprès d'un portail d'identification.

Au sein du protocole SAML, on distingue deux entités :

- IdP (Identity Provider) : Le gestionnaire d'identités, qui gère l'authentification et est garant de l'authenticité d'une personne et des informations qui lui sont liées. Les gestionnaires suivants sont parmi les plus connus : Microsoft ADFS (via Active Directory), Azure AD, Okta et Auth0.
- SP (Service Provider) : Le fournisseur de service qui va déléguer l'authentification à l'IdP. Il s'agit du serveur Akuiteo.

Note

Le protocole SAML prévoit deux grands types d'opérations : l'Authentication et le Provisioning. Le Provisioning, qui sert à créer et alimenter un utilisateur non connu, n'est pas géré par Akuiteo.

4.3.1 Prérequis

Important

Le Portail Collaborateur et le Portail Client ne peuvent en aucun cas remplacer le rôle de SP. L'accès au serveur Akuiteo est donc obligatoire.

Comme le SP est le serveur Akuiteo, l'utilisateur doit avoir accès aux adresses suivantes :

- /akuiteo/login.html
- /akuiteo/routing.html
- /akuiteo/saml/SSO
- /akuiteo/saml/logout

De plus, le code utilisateur doit être l'adresse mail de l'utilisateur.

4.3.2 Préparer la configuration

Créer un magasin de certificats

Note

Cette étape n'est pas nécessaire pour les clients en SaaS.

Le serveur Akuiteo doit disposer d'un fichier de certificat au format .jks afin de crypter les échanges avec l'IdP. Pour cela, nous utilisons l'utilitaire Java Keytool afin de créer un certificat auto-signé.

1 Sur le serveur Akuiteo, exécutez la commande suivante :

```
keytool -genkey -keyalg RSA -alias saml -keystore saml.jks -keysize 2048
```

- 2 Renseignez les informations principales du certificat et conservez bien le mot de passe du fichier.
L'extrait suivant est un exemple :

```
Quels sont vos nom et prénom ?
[Unknown]: Akuiteo
Quel est le nom de votre unité organisationnelle ?
[Unknown]: IT
Quel est le nom de votre entreprise ?
[Unknown]: Akuiteo
Quel est le nom de votre ville de résidence ?
[Unknown]: Lyon
Quel est le nom de votre état ou province ?
[Unknown]: Rhône
Quel est le code pays à deux lettres pour cette unité ?
[Unknown]: FR
Est-ce CN=Akuiteo, OU=IT, O=Akuiteo, L=Lyon, ST=Rhône, C=FR ?
[non]: oui

Entrez le mot de passe de la clé pour <saml>
      (appuyez sur Entrée s'il s'agit du mot de passe du fichier de clés) :
Ressaisissez le nouveau mot de passe :

Warning:
Le fichier de clés JKS utilise un format propriétaire. Il est recommandé de migrer vers
PKCS12, qui est un format standard de l'industrie en utilisant "keytool -importkeystore -
srckeystore saml.jks -destkeystore saml.jks -deststoretype pkcs12".
```

↳ Un fichier `saml.jks` est généré. Ce fichier sera utilisé par la suite dans la configuration Akuiteo.

Modifier la configuration Tomcat

- 1 Depuis le répertoire d'installation Tomcat du serveur Akuiteo, allez dans **conf**.
- 2 Ouvrez le fichier de configuration **context.xml** avec un éditeur de texte.
- 3 Enlevez le commentaire du tag `<Manager ... />` comme suit :

```
<Context>

    <!-- Default set of monitored resources -->
    <WatchedResource>WEB-INF/web.xml</WatchedResource>

    <!-- Uncomment this to disable session persistence across Tomcat restarts -->
    <Manager pathname="" />

    <!-- Uncomment this to enable Comet connection tacking (provides events
         on session expiration as well as webapp lifecycle) -->
    <!--
    <Valve className="org.apache.catalina.valves.CometConnectionManagerValve" />
    -->

</Context>
```

- 4 Redémarrez le serveur Tomcat pour que la modification soit prise en compte.

Renseigner l'URL externe du serveur Akuiteo

Lors d'une phase de connexion SAML, le Portail Collaborateur et le Portail Client effectuent une redirection vers le serveur Akuiteo afin d'initier la connexion SAML. Les portails doivent donc connaître l'adresse externe / publique du serveur Akuiteo.

Pour cela, deux solutions sont possibles :

- Ajoutez un élément de configuration pour chaque portail.
- Dans le fichier de configuration **context.xml**, ajoutez :

```
<!-- SAML -->
<Environment name="t9gestion#t9gest.extrenal.server.url" type="java.lang.String"
override="false" value="https://akuiteo.myakuiteo.com/akuiteo"/>
```

Limiter l'authentification SAML à certains domaines mail

Lorsque l'authentification SAML est activée, tout identifiant mail est redirigé par défaut vers l'IdP afin d'être authentifié.

Si vous souhaitez limiter cette authentification à certains domaines mail, ajoutez le paramètre `saml.domains` (lié au serveur métier) dans le fichier de configuration **context.xml**. Ce paramètre vous permet de spécifier :

- soit un seul domaine,
- soit une liste de domaines, séparés par une virgule (,).

Par exemple :

```
<!-- SAML -->
<Environment name="t9-gestion#saml.domains" type="java.lang.String" override="false"
value="akuiteo.com, myakuiteo.com"/>
```

Aligner le secret JWT entre les portails web et le serveur Akuiteo

Si le serveur Akuiteo et le ou les portails web sont hébergés sur des instances Tomcat séparées, vous devez "aligner" le secret JWT, c'est-à-dire harmoniser ce secret entre chaque instance. Ce secret est utilisé pour le cryptage des identifiants collaborateurs entre les différents serveurs Akuiteo. Un secret de 63 caractères alphanumériques est suffisant.

Astuce

Pour générer le secret JWT, vous pouvez utiliser un générateur (par exemple <https://www.grc.com/passwords.htm>).

Renseignez le secret dans les paramètres JVM de chaque Tomcat en ajoutant :

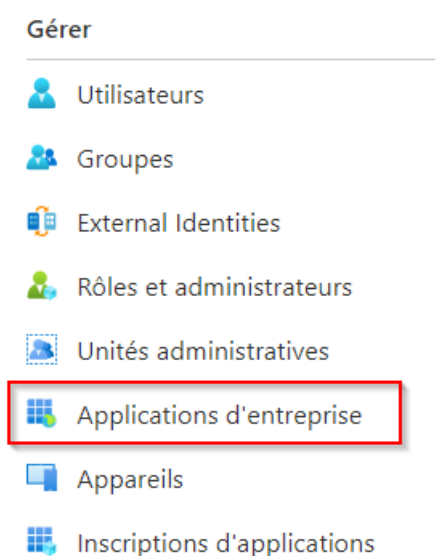
```
-Djwt.secret=iUFmfacoxwH4dzGzd2UxcNsvuebt8rI0wupyN371EREB0uP02x2xzPZuRFjDn0W
```

4.3.3 Créer une application SAML

Note

La configuration avec Azure AD représente le cas le plus courant. La procédure qui suit décrit la création d'une application SAML depuis le portail Azure AD, mais un autre gestionnaire d'identités peut être utilisé.

- 1 Dans un navigateur web, entrez l'adresse <https://portal.azure.com/> et connectez-vous en tant qu'administrateur. Sur la page d'accueil, cliquez sur le bouton **Voir** dans la section **Gérer Azure Active Directory**.
- 2 Cliquez sur **Applications d'entreprise** dans le menu de gauche, puis cliquez sur **Nouvelle application** depuis l'entête de la page des applications.



- 3 Cliquez ensuite sur **Créer votre propre application**.

Parcourir la galerie Azure AD ...



La galerie Azure AD App est un catalogue de milliers d'applications qui facilitent le déploiement de nouvelles applications, vous tirez parti de modèles prédéfinis pour connecter vos utilisateurs

- 4 Renseignez le **Nom** de cette nouvelle application (par exemple *Akuiteo-Production*) et laissez l'option **Integrate any other application you don't find in the gallery (Non-gallery)** cochée. Cliquez ensuite sur **Créer**.
- 5 Sur la page de la nouvelle application, sélectionnez le bloc **2. Configurer l'authentification unique** puis sélectionnez le bloc **SAML**.

6 Dans la page de configuration de l'authentification, renseignez les champs obligatoires :

- **Identificateur (ID d'identité)** - URL de votre serveur Akuiteo, par exemple :
https://akuiteo.myakuiteo.com/akuiteo
- **URL de réponse** - URL de connexion SAML basée sur l'URL précédente (suffixée par /saml/SSO), par exemple : *https://akuiteo.myakuiteo.com/akuiteo/saml/SSO*

Configurer l'authentification unique avec SAML

Une implémentation SSO basée sur les protocoles de fédération améliore la sécurité, la fiabilité et l'expérience de l'utilisateur final. Elle est également plus facile à implémenter. Choisissez l'authentification unique SAML chaque fois que cela est possible pour les applications existantes qui n'utilisent pas OpenID Connect ou OAuth. [En savoir plus.](#)

Lire le [guide de configuration](#) pour l'intégration de Akuiteo-Production.

1

Configuration SAML de base

Modifier

Identificateur (ID d'entité)	Obligatoire
URL de réponse (URL Assertion Consumer Service)	Obligatoire
URL de connexion	<i>Facultatif</i>
État du relais (facultatif)	<i>Facultatif</i>
URL de déconnexion (facultatif)	<i>Facultatif</i>

2

Attributs et revendications

⚠ Remplir les champs requis à l'étape 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname

4.3.4 Configurer la Console d'administration

Coté Akuiteo, les informations de configuration SAML sont définies dans la Console d'administration, depuis le menu **Sécurité > SAML**.

- 1 Depuis l'écran **Configurations SAML**, cliquez sur le bouton **Créer une nouvelle configuration** en haut à droite de l'écran.
- 2 Dans la fenêtre de configuration, renseignez les champs suivants :

Champ	Description
Code	Attribuez un code à la configuration pour l'identifier. Ce code doit être unique.
Configuration active	Cochez cette case pour activer l'authentification avec SAML. Si la case n'est pas cochée, l'authentification sera fondée sur une autre méthode d'authentification (si activée) ou sur la base de données.
IDP	Renseignez le champ identificateur de l'IdP.

Champ	Description
	Si vous utilisez Active Directory, il s'agit de l' Identificateur Azure AD .
Audience	Renseignez l'identifiant de l'application auprès de l'IdP et l'URL publique. Si vous utilisez Active Directory, il s'agit de l' Identificateur (ID d'identité) .
MetaLocation	Renseignez l'emplacement du fichier de metadata (URL ou fichier local). Si vous utilisez Active Directory, il s'agit de l'URL des métadonnées de fédération d'applications.
KeyAlias	Renseignez l'alias du fichier de certificat (.jks).
KeyPwd	Renseignez le mot de passe du fichier de certificat (.jks).
KeyLocation	Renseignez l'emplacement du fichier de certificat (.jks).

Note


Les fichiers MetaLocation et KeyLocation ont une notation "URL" : le protocole doit donc être spécifié en entête. Dans le cas d'un fichier stocké en local, faites précéder le chemin par **file:/**.

3 Cliquez sur **Enregistrer**.

↳ Si la connexion est établie, la configuration est ajoutée dans la Console d'administration. Si la connexion ne peut pas être établie, un message d'erreur est affiché.

4 Redémarrez le serveur pour que la configuration soit prise en compte.

Pour modifier une configuration, cliquez sur  pour la ligne concernée, modifiez les informations souhaitées puis cliquez sur **Mettre à jour**.

Pour supprimer une configuration, cliquez sur  pour la ligne concernée et confirmez la suppression.

4.4 CONFIGURER L'AUTHENTIFICATION OAUTH2

L'authentification Oauth2 est uniquement utilisée par Akuteo dans le contexte des APIs. Cette authentification permet d'identifier les différents clients (c'est-à-dire les applications tierces) qui souhaitent accéder à une ressource.

Les informations de configuration Oauth2 sont définies dans la Console d'administration, depuis le menu **Sécurité > Oauth2**.

1 Depuis l'écran **Clients autorisés**, cliquez sur le bouton **Créer un nouveau client** en haut à droite de l'écran.


2 Dans la fenêtre de configuration, renseignez les champs suivants :

Champ	Description
Client ID	Renseignez le Client ID utilisé pour l'authentification Oauth.

Champ	Description
Durée (s)	Renseignez la durée de validité, en secondes, de l'access token.
Durée refresh (s)	Le refresh token permet de demander un nouvel access token sans avoir à renseigner à nouveau les identifiants. Renseignez la durée de validité, en secondes, de ce refresh token, c'est-à-dire la durée pendant laquelle le refresh token pourra être utilisé pour demander un nouvel access token.
Scope	Renseigner read_write . Les autorisations étant basées sur les DMF, vous pouvez donner accès au scope read_write pour lire, modifier et supprimer les ressources.

3 Cliquez sur **Créer**.

↳ Le client est ajouté dans la Console d'administration. Akuiteo vous fournit un Client **Secret** associé à ce nouveau client, à utiliser dans les appels aux APIs.

Pour modifier un client, cliquez sur  pour la ligne concernée, modifiez les informations souhaitées puis cliquez sur **Mettre à jour**.

Pour supprimer un client, cliquez sur  pour la ligne concernée et confirmez la suppression.

Référence

Pour plus d'informations sur les APIs d'Akuiteo, référez-vous à la [Documentation des APIs](#).