



Guide de paramétrage

CONSOLE D'ADMINISTRATION

Version 4.5

Numéro de révision : 4

Date de publication : février 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	Configurer Akuiteo depuis la Console d'Administration	5
2.1	Configurer l'OCR	5
2.2	Configurer la connexion à l'API SIRENE	6
2.2.1	Ajouter le certificat Certigna au serveur Tomcat	6
2.2.2	Paramétrer la Console d'administration	7
2.3	Configurer la connexion au serveur Exchange	7
2.4	Configurer la dématérialisation des factures	10
2.5	Configurer la signature électronique	11

1 Préface

1.1 RÉVISIONS

Révision 4	Publiée en février 2023 <ul style="list-style-type: none">• Ajout des paramètres liés à l'authentification OAUTH dans Configurer la connexion au serveur Exchange (p. 7).
Révision 3	Publiée en août 2022 <ul style="list-style-type: none">• Mise à jour du sous-chapitre Ajouter le certificat Certigna au serveur Tomcat (p. 6).
Révision 2	Publiée en décembre 2021 <ul style="list-style-type: none">• Précision des API Sirene et Métadonnées pour Configurer la connexion à l'API SIRENE (p. 6).• Mise à jour globale du chapitre Configurer la dématérialisation des factures (p. 10).
Révision 1	Publiée en juin 2021 <ul style="list-style-type: none">• Ajout du chapitre Configurer la connexion à l'API SIRENE (p. 6).

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 Configurer Akuiteo depuis la Console d'Administration

2.1 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.

2.2 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 ou d'un client 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.

2.2.1 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.

2.2.2 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.

2.3 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.

2.4 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.

Le paramétrage de la Console d'administration est effectué pour une seule structure CHORUS PRO.

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.
Identifiant Client	Renseignez l'identifiant client permettant de s'authentifier à CHORUS PRO. Cet identifiant est récupéré depuis le compte PISTE.
Secret	Renseignez le mot de passe permettant de s'authentifier à CHORUS PRO. Ce mot de passe est lié à l'identifiant récupéré depuis le compte PISTE.
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.
Login Chorus	Renseignez le login du compte technique CHORUS PRO.
Mot de passe Chorus	Renseignez le mot de passe associé au login du compte technique CHORUS PRO.
Identifiant	Renseignez l'identifiant de la structure CHORUS PRO rattachée au compte technique.
Liste de CODE de dématérialisations valides	Renseignez le code de dématérialisation CHORUS_DEMATERIALIZED accepté par les APIs CHORUS PRO.

Important

Les champs **URL Authentication Chorus**, **Identifiant Client**, **Secret** et **Url** doivent être différents entre un environnement de production et de test.

2 Renseignez les champs suivants pour configurer l'interface avec 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 l'utilisateur Akuiteo	Renseignez le code de la société de connexion.
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>

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.
- 4 Cliquez sur le bouton **Tester** pour tester la connexion à CHORUS PRO à partir des valeurs renseignées.

2.5 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> <div>Note Il est déconseillé de renseigner un intervalle trop bas pour ne pas surcharger les appels.</div>
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 Akuteo.</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.