



akuiteo
BUSINESS SOFTWARE

Setup Guide

ADMINISTRATION CONSOLE

Version 4.5

Revision number: 4

Published in: February 2023

Written by: Documentation team

Copyright (c) 2006-2023 Akuiteo S.A.S. All Rights Reserved.

Any total or partial reproduction of this material, whether its form or content, without prior written permission from the author, is strictly prohibited. The French law only allows, on one hand, copies or reproductions strictly reserved for private usage of the copyist and not destined for collective usage and, on the other hand, analysis and short quotes for the purpose of illustration.

The Akuiteo designation and logos are registered trademarks of the Akuiteo S.A.S. company. Any use of the trademarks without the authorization of the Akuiteo S.A.S. company is prohibited.

Visit: <http://www.akuiteo.com> and <http://www.akuiteo.com/blog/>

Table of Contents

1 Preface	4
1.1 Revisions	4
1.2 Help desk	4
2 Configuring Akuiteo from the Administration console	5
2.1 Configuring OCR	5
2.2 Configuring the SIRENE API	6
2.2.1 Adding the Certigna certificate to the Tomcat server	6
2.2.2 Setting up the Administration console	7
2.3 Configuring the connection to the Exchange server	7
2.4 Configuring the dematerialization of invoices	9
2.5 Configuring electronic signatures	11

1 Preface

1.1 REVISIONS

Revision 4	Published in February 2023 <ul style="list-style-type: none">Added parameters linked to the OAUTH authentication in Configuring the connection to the Exchange server (p. 7).
Revision 3	Published in August 2022 <ul style="list-style-type: none">Updated the Adding the Certigna certificate to the Tomcat server (p. 6) sub-chapter.
Revision 2	Published in December 2021 <ul style="list-style-type: none">Details about the Sirene and Métadonnées APIs for Configuring the SIRENE API (p. 6).Global update for the Configuring the dematerialization of invoices (p. 9) chapter.
Revision 1	Published in June 2021 <ul style="list-style-type: none">Added chapter Configuring the SIRENE API (p. 6).

1.2 HELP DESK

Akuiteo S.A.S. highly values your satisfaction.

To share your feedback or contact the help desk, feel free to visit our website page:

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

2 Configuring Akuiteo from the Administration console

2.1 CONFIGURING OCR

OCR (Optical Character Recognition) is a technology used to convert different types of documents, such as scanned paper documents, PDF files or numeric photos, into modifiable and searchable files. An OCR software is able to recognize letters included in images, and to build entire words or sentences with these letters.

Akuiteo integrates an OCR feature to simplify the process of adding expenses to an expense report from the Web Portal and the Akuiteo Mobile application. When a receipt is photographed, the characters are automatically recognized and are then added in the expense's relevant fields.

OCR is configured from the Administration console, from the **Configuration > OCR** menu.

- 1 In the **OCR configuration** screen, select **OCR_MINDEE** from the drop-down list of the **provider** field.
- 2 Fill in the following fields to configure OCR:

Field	Description
OCR Activated	Check this box to globally activate OCR.
Mindee Activated	Check this box to activate Mindee's OCR on the Web Portal and the Akuiteo Mobile application.
Mindee rest url	Specify the URL to connect to the web service, provided by Akuiteo.
Mindee Token	Fill in the token provided by Akuiteo to access the web service.
Akuiteo user	Fill in the Akuiteo login to connect to the web service. This user makes it possible to differentiate expenses generated with OCR from the ones added by employees. When an expense is generated with OCR, the Akuiteo user is specified in the expense's history.
Akuiteo password	Fill in the password associated with the Akuiteo login.

- 3 Click on **Save** for each field that is filled in or modified to take into account the value specified.
- 4 Click on the **Test** button to test the connection to Mindee's OCR interface using the values specified.

2.2 CONFIGURING THE SIRENE API

The SIRENE API is used to automatically fill in the relevant fields when creating a prospect or a customer thanks to the specified SIRET or SIREN number. If the SIRET or SIREN number specified is known by the SIRENE API, the relevant fields (such as the call name or the address) will be filled in automatically.

2.2.1 Adding the Certigna certificate to the Tomcat server

The Java Runtime Environment (JRE) has a configuration file (keystore) that includes root certificates from the different renowned certification authorities. When a connection is established to another system using https, this list of certificates is used to validate the secured connection.

Some certification authorities are not included in the file provided by default with the JRE, so they must be added manually. In the SIRENE API's context, you must add the Certigna certificate to certify connections.

Note

For SaaS customers, this certificate is added by Akuiteo.

Identifying the JRE's location

- 1 Connect to the server that hosts the Akuiteo environment.
- 2 Launch the Tomcat Manager for that environment.
- 3 From the **Java** tab, take note of the location of the JRE used by Tomcat.

Retrieving the Certigna's Racine certificate

- 1 Go to the Certigna's website: <https://www.certigna.com/autorite-crl>.
- 2 Download the Certigna's authority certificate: *certigna.der*.

Importing the certificate into the JRE's keystore

- 1 Launch the command prompt as an administrator.
- 2 Launch the following command:

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

In this command, you must replace:

- **[JRE_LOCATION]** with the location of the JRE used by Tomcat
- **[CERTIFICATE_LOCATION]** with the location of the *certigna.der* certificate downloaded.

Example

```
"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
```

- Restart the Tomcat server of the targeted Akuiteo environment to take into account the new certificate.

2.2.2 Setting up the Administration console

The connection to the SIRENE API is configured from the Administration Console, from the **Configuration > API Sirene** menu.

- Fill in the following fields to configure the connection:

Field	Description
SIRENE API use	Check the box to use the SIRENE API.
Token for SIRENE API	Fill in the token generated from the api.insee.fr website. To retrieve that token: <ol style="list-style-type: none">As an administrator, create an account on the api.insee.fr website.Activate the Sirene and Métadonnées APIs for the application (Akuiteo).Generate a token for this application, no matter the number of APIs interrogated, and define the validity period for this token.

- Click on **Save** for each field that is filled in or modified to take into account the value specified.
- Click on the **Test** button to test the connection to the SIRENE API using the values specified.

2.3 CONFIGURING THE CONNECTION TO THE EXCHANGE SERVER

The connection parameters to the Exchange server are used to synchronize schedules or appointments from Akuiteo into a Microsoft Outlook calendar.

The connection to the Exchange server is configured from the Administration Console, from the **Configuration > Exchange** menu.

- Fill in the following fields to configure the connection to the Exchange server:

Field	Description
Delegated user	Fill in the login of the Exchange user to connect to the server. If you are using Exchange 365, this user must have a delegation to have complete access over other user accounts.

Field	Description						
Linked password	Specify the password associated with the login of the Exchange user.						
EWS service URL	<p>Fill in the URL to connect to the Exchange server.</p> <div> <p>Example</p> <p>https://outlook.office365.com/EWS/exchange.asmx</p> </div>						
Exchange server version	Select the Exchange server version from the drop-down list.						
Maximum number of threads for synchronizing	Specify a maximum number for simultaneous synchronizations.						
Use optimized library for Office 365	If you are using Exchange 365, check this box to use the library optimized for Office 365.						
Use impersonation	<p>If you are using Exchange 365, check this box. Office 365 enforces a limit on the number of web service calls a given user can make. Impersonation is used to assign a role to an Exchange user and bypass this limit.</p> <p>To be able to use impersonation, you must:</p> <p>Delete all account delegations for the Exchange technical user</p> <ol style="list-style-type: none"> Download and install PowerShell. From PowerShell, run the following command lines: <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>This command establishes a connection to the Exchange server. The administrator's login and password are required.</td></tr> <tr> <td> <pre>Import-PSSession \$Session</pre> </td><td>This command gathers the commands needed to delete delegations.</td></tr> <tr> <td> <pre>foreach (\$mailbox in Get-Mailbox) { Remove-MailboxPermission \$mailbox.PrimarySmtpAddress -user user@domain -Accessright FullAccess -Confirm: \$false}</pre> </td><td> <p>Replace user@domain with the login of the current Akuiteo technical user who owns the delegation right.</p> <p>This command deletes the delegation role for all users.</p> </td></tr> </table> <p>Give the impersonation right to the Exchange technical user</p> <ol style="list-style-type: none"> Connect to the Exchange Admin Center from the Office 365 portal. 	<pre>\$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential \$UserCredential -Authentication Basic -AllowRedirection</pre>	This command establishes a connection to the Exchange server. The administrator's login and password are required.	<pre>Import-PSSession \$Session</pre>	This command gathers the commands needed to delete delegations.	<pre>foreach (\$mailbox in Get-Mailbox) { Remove-MailboxPermission \$mailbox.PrimarySmtpAddress -user user@domain -Accessright FullAccess -Confirm: \$false}</pre>	<p>Replace user@domain with the login of the current Akuiteo technical user who owns the delegation right.</p> <p>This command deletes the delegation role for all users.</p>
<pre>\$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential \$UserCredential -Authentication Basic -AllowRedirection</pre>	This command establishes a connection to the Exchange server. The administrator's login and password are required.						
<pre>Import-PSSession \$Session</pre>	This command gathers the commands needed to delete delegations.						
<pre>foreach (\$mailbox in Get-Mailbox) { Remove-MailboxPermission \$mailbox.PrimarySmtpAddress -user user@domain -Accessright FullAccess -Confirm: \$false}</pre>	<p>Replace user@domain with the login of the current Akuiteo technical user who owns the delegation right.</p> <p>This command deletes the delegation role for all users.</p>						

Field	Description
	<p>2. Go to the Permissions > Admin Roles menu.</p> <p>3. Create a new role by filling the following information:</p> <ul style="list-style-type: none"> • Name: Application Impersonation • Assigned roles: Add the ApplicationImpersonation, Legal Hold and Mailbox Search roles • Members: Add the current Akuiteo technical user
Test user	Specify an existing email address to make sure that Akuiteo can access the corresponding account using the impersonation.
Use OAUTH authentication (Exchange 365 only)	<p>Enable or disable OAUTH authentication to connect to Exchange.</p> <p>This option must be enabled if Exchange 365 is used by Akuiteo in your organization. Otherwise, it must be disabled.</p>
Tenant ID	<p>This field must be entered if Use OAUTH authentication (Exchange 365 only) is enabled.</p> <p>Enter the tenant ID provided by Microsoft for the OAUTH authentication.</p>
Client ID	<p>This field must be entered if Use OAUTH authentication (Exchange 365 only) is enabled.</p> <p>Enter the client ID for the OAUTH authentication.</p>
Client Secret	<p>This field must be entered if Use OAUTH authentication (Exchange 365 only) is enabled.</p> <p>Enter the client secret for the OAUTH authentication.</p>

2 Click on **Save** for each field that is filled in or modified to take into account the value specified.

3 Click on the **Test** button to test the connection to the Exchange interface using the values specified.

2.4 CONFIGURING THE DEMATERIALIZATION OF INVOICES

The configuration parameters for CHORUS PRO are used to automatically transfer the dematerialized invoices generated by Akuiteo to the CHORUS PRO portal. It makes it possible to generate and then automatically transfer dematerialized invoices from the Application Desktop, without having to use an external tool or to transfer the invoices manually.

The automatic transfer of dematerialized invoices is set up from the Administration Console, from the menu **Configuration > Dematerialization**.

Notes

For SaaS customers, the setup of the Administration console is done by Akuiteo.

The setup of the Administration console is done for a single CHORUS PRO structure.

1 Fill in the following fields to configure the connection to CHORUS PRO:

Field	Description
Chorus Active	Check this box to activate the connection to CHORUS PRO.
Chorus Authentication URL	Specify the URL to authenticate to CHORUS PRO: <ul style="list-style-type: none">• https://sandbox-oauth.aife.economie.gouv.fr/api/oauth/token for test environments,• https://oauth.aife.economie.gouv.fr/api/oauth/token for production environments.
Customer ID	Specify the customer ID allowing the authentication to CHORUS PRO. This ID is retrieved from the PISTE account.
Secret	Specify the password allowing the authentication to CHORUS PRO. This password is linked to the ID retrieved from the PISTE account.
Url	Specify the URL to connect to CHORUS PRO: <ul style="list-style-type: none">• https://sandbox-api.aife.economie.gouv.fr/ for test environments,• https://api.aife.economie.gouv.fr/ for production environments.
Chorus Login	Specify the login from the CHORUS PRO technical account.
Chorus password	Specify the password associated with the login from the CHORUS PRO technical account.
ID	Specify the ID of the CHORUS PRO structure linked to the technical account.
List of valid dematerialization CODES	Specify the CHORUS_DEMATERIALIZED code, which can be used by the CHORUS PRO APIs.

Important

The **Chorus Authentication URL**, **Customer ID**, **Secret** and **Url** fields must be different if it is a production or a test environment.

2 Fill in the following fields to configure the interface with CHORUS PRO:

Field	Description
Akuiteo user	Specify the login of the Akuiteo's technical user.
Akuiteo user's password	Specify the password associated with the Akuiteo login.
Akuiteo user's company	Specify the code of the company used for connection.

Field	Description
code	
Number of successive test runs in case of an error	<p>The number of successive test runs enables to specify, in case of an error when transferring dematerialized invoices, the number of times that Akuiteo will re-run the transfer.</p> <p>By default, Akuiteo performs 3 successive test runs in case of an error.</p>
Time period in seconds between two successive test runs	<p>The time period between two successive test runs enables to specify, in seconds, the waiting period before another transfer is attempted in case of an error.</p> <p>By default, Akuiteo waits 10 seconds between two successive test runs</p>

Note

The CHORUS PRO portal has quotas for transferring dematerialized invoices:

- On the test environment: 5 queries per second with a maximum of 50,000 queries per day
- On the production environment: 20 queries per second with a maximum of 1 million queries per day

When these quotas are reached, the invoices can no longer be transferred. You should adapt the values in the **Number of successive test runs in case of an error** and **Time period in seconds between two successive test runs** fields if you regularly have errors when transferring invoices.

- 3 Click on **Save** for each field that is filled in or modified to take into account the value specified.
- 4 Click on the **Test** button to test the connection to CHORUS PRO using the values specified.

2.5 CONFIGURING ELECTRONIC SIGNATURES

The configuration parameters of the Universign APIs are used for signing quotations and sales delivery notes electronically. Using these APIs makes it possible to send quotations and delivery notes out for electronic signature directly from the Application Desktop, without having to use an additional interface.

The electronic signature is configured from the Administration Console, from the **Configuration > Electronic signature** menu.

- 1 Fill in the following fields to configure the electronic signature:

Field	Description
Activate electronic signature	Check this box to activate the electronic signature.
Universign URL	Specify the URL provided by Akuiteo to connect to the Universign APIs.
Universign	Fill in the login of the Universign user, provided by Akuiteo.

Field	Description
user	
Universign password	Specify the password associated with the login of the Universign user, provided by Akuiteo.
Akuiteo user	Fill in the login of the Akuiteo technical user, used to connect to the APIs.
Akuiteo password	Specify the password associated with the login of the Akuiteo technical user.
Time range for retrieving signatures	<p>A scheduled task is executed as a background task to search for signature statuses (whether the recipients for electronic signing have signed or not) and, once all signatures have been made, to retrieve the signed documents.</p> <p>The time range for retrieving signatures is used to define, in seconds, the time range for executing this scheduled task.</p> <p>By default, the task is executed every 21600 seconds, that is to say every 6 hours.</p> <div> <p>Note</p> <p>It is not recommended to specify a small time range so as to not overload the calls.</p> </div>
Start period	<p>The start period is used to define, in seconds, the time before executing the first scheduled task after the Akuiteo server has been launched.</p> <p>By default, the task is executed for the first time 20 seconds after the server is launched.</p>

- 2** Click on **Save** for each field that is filled in or modified to take into account the value specified.
- 3** Click on the **Test** button to test the connection to the Universign APIs using the values specified.