



akuiteo
BUSINESS SOFTWARE

Setup Guide

ADMINISTRATION CONSOLE

Version 4.6

Revision number: 6

Published in: August 2022

Written by: Documentation team

Copyright (c) 2006-2022 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 Accessing the Administration console	5
2.1 Logging in to the console	5
2.2 Changing the language	5
2.3 Changing the theme	5
2.4 Logging out of the console	5
3 Configuring Akuiteo from the Administration console	6
3.1 Configuring OCR	6
3.2 Configuring the SIRENE API	7
3.2.1 Adding the Certigna certificate to the Tomcat server	7
3.2.2 Setting up the Administration console	8
3.3 Configuring the connection to the Exchange server	8
3.4 Configuring the dematerialization of invoices	10
3.5 Configuring electronic signatures	11
3.6 Configuring Akuiteo Connect	12
4 Configuring authentication methods	15
4.1 Configuring the LDAP authentication	15
4.1.1 Prerequisites	15
4.1.2 Configuring the Administration console	15
4.2 Configuring the Azure AD authentication	17
4.2.1 Accessing the Azure portal	17
4.2.2 Registering Akuiteo in the Azure AD's directory	17
4.2.3 Creating a "client secret" to identify the Akuiteo server	19
4.2.4 Allowing the Akuiteo application	19
4.2.5 Configuring the Administration console	20
4.3 Configuring the SAML authentication	21
4.3.1 Prerequisites	21
4.3.2 Preparing the configuration	21
4.3.3 Creating a SAML application	24
4.3.4 Configuring the Administration console	25
4.4 Configuring the Oauth2 authentication	26

1 Preface

1.1 REVISIONS

Revision 6	Published in August 2022 <ul style="list-style-type: none">Updated the Adding the Certigna certificate to the Tomcat server (p. 7) sub-chapter.
Revision 5	Published in May 2022 <ul style="list-style-type: none">Forgotten password can now be retrieved (see Logging in to the console (p. 5)).
Revision 4	Published in April 2022 <ul style="list-style-type: none">Added chapter Configuring authentication methods (p. 15).
Revision 3	Published in February 2022 <ul style="list-style-type: none">Sirene API taken into account when creating suppliers (see Configuring the SIRENE API (p. 7)).
Revision 2	Published in January 2022 <ul style="list-style-type: none">Details about the Sirene and Métadonnées APIs for Configuring the SIRENE API (p. 7).
Revision 1	Published in November 2021 <ul style="list-style-type: none">Added chapter Accessing the Administration console (p. 5).Updated sub-chapter Configuring the dematerialization of invoices (p. 10) for the multi-company.Added the Configuring Akuiteo Connect (p. 12) sub-chapter.

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 Accessing the Administration console

2.1 LOGGING IN TO THE CONSOLE

- 1 In a web browser, enter the address in the following format:
https://domainname/servername/apps/admin/ or open the Launcher to access the Administration console.

Example

https://www.akuiteo.com/akuiteo/apps/admin/

Note

To access the Administration console from the Launcher, the link to the application must have been initialized from the console. For more information, refer to the *General Guide - Launcher*.

- 2 In the login window, fill in the **Login** and the **Password**.

- 3 Click on **Log in**.

↳ The Administration console's home page opens.

Tip

Did you forget your password? In the login window, fill in the login in the **User** field and click **Forgot your password?**, then confirm the password reset. An email will be sent so that you modify your login credentials.

2.2 CHANGING THE LANGUAGE

To change the interface's language, click on the connected user's picture in the header then click on the flag for the desired language. The interface is automatically changed in the selected language.

2.3 CHANGING THE THEME

To change the color theme of the interface, click on the connected user's picture in the header, then click on the Dark or Light theme. The interface automatically displays the selected theme.

2.4 LOGGING OUT OF THE CONSOLE

To log out from the console, click on the connected user's picture in the header, then click on **Logout**.

3 Configuring Akuiteo from the Administration console

3.1 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.

3.2 CONFIGURING THE SIRENE API

The SIRENE API is used to automatically fill in the relevant fields when creating a prospect, a customer or a supplier 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.

3.2.1 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.

3.2.2 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.

3.3 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.

- 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.

3.4 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.

Reference

The login information to CHORUS PRO must be specified from the setup of the Application Desktop to enable you to use different CHORUS PRO accounts depending on each company. For more information, refer to the *Setup Guide - Chorus Dematerialization*.

- 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	<p>Specify the URL to authenticate to CHORUS PRO:</p> <ul style="list-style-type: none"> • https://sandbox-oauth.aife.economie.gouv.fr/api/oauth/token for test environments,

Field	Description
	<ul style="list-style-type: none"> • https://oauth.aife.economie.gouv.fr/api/oauth/token for production environments.
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.

2 Fill in the following fields to configure the interface between Akuiteo and 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 code	Specify the code of the company used for connection.
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>
Maximum number of calls to Chorus per second	<p>Specify a maximum number of simultaneous calls to CHORUS PRO per second.</p> <p>By default, there is a maximum of 20 calls per second. For a test environment, the number must be set on maximum 1 call per second.</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.

3.5 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 user	Fill in the login of the Universign user, provided by Akuiteo.
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>Note It is not recommended to specify a small time range so as to not overload the calls.</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.

3.6 CONFIGURING AKUITEO CONNECT

Configuration parameters for Akuiteo Connect are used to connect to the Bridge connector in order to automatically and securely retrieve bank transactions in Akuiteo. The Bridge connection makes it possible to retrieve bank transactions directly from your bank, without having to manually import bank

statement files.

The connection to Akuiteo Connect is configured from the Administration Console, from the **Configuration** > Akuiteo **Connect** menu.

Important

First, Akuiteo must set up the login information of your Bridge account in order for you to activate and configure Akuiteo Connect.

Configuring the connection to Akuiteo Connect

1 In the **Akuiteo Connect** section, fill in the following fields to configure the connection:

Field	Description
Activate Akuiteo Connect	Check this box to activate the connection to Akuiteo Connect.
Akuiteo user	Specify the login of the Akuiteo's technical user. This user will be used to create new statements from retrieved bank transactions.
Akuiteo password	Specify the password associated with the Akuiteo login.
Email	Enter the email address to which execution logs of the scheduled task will be sent.
Time range for retrieving statements	<p>A scheduled task is executed as a batch process to retrieve transactions from the connected bank accounts. The transactions are stored in an intermediate table until a statement is generated.</p> <p>The time range for retrieving statements is used to define, in seconds, the time range for executing this scheduled task.</p> <p>By default, the task is executed every 21,600 seconds.</p> <div>Note It is not recommended to specify a small time range so as to not overload the calls.</div>
Start period (20s by default)	<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 Akuiteo Connect using the values specified.

Adding a Bridge user

Note

You can only add one Bridge user. Indeed, an Akuiteo customer is associated with only one Bridge account/user.

The user of the account created from Bridge must be added to the Administration console to link the bank accounts associated with that Bridge user in Akuiteo. This Bridge user is namely linked to the bank accounts of all the companies; however, access to these bank accounts remains subject to the authentication of each account's owner.

- 1 In the **Bridge user** section, click on **New Bridge user**.
- 2 In the window, fill in the **Name**, **Email** and **Password** used to create the Bridge account.
- 3 Click on **Create**.

↳ The Bridge user is added to the Administration console.

To modify the user information, click on , modify the desired information then click on **Update**.

To delete the user, delete all the associated banks then click on  and confirm the deletion.

4 Configuring authentication methods

Akuiteo enables you to manage user authentication with several methods:

- The Akuiteo-based authentication, that is not explained in this chapter. Users and their associated password are set up in the Application Desktop and are stored in the database.
- The LDAP authentication, where users are declared in an LDAP directory (Active Directory for example). Refer to [Configuring the LDAP authentication \(p. 15\)](#).
- The Azure Active Directory authentication, a service provided by Microsoft for all Office 365 customers. Refer to [Configuring the Azure AD authentication \(p. 17\)](#).
- The SAML (Security Assertion Markup Language) authentication, an open standard that makes it possible to use a single authentication on an identification portal for various applications. SAML is standardized and can therefore work with the product used in your company (Azure AD or Okta for example). Refer to [Configuring the SAML authentication \(p. 21\)](#).
- The OAuth2 authentication, only used to make calls to Akuiteo's APIs. Refer to [Configuring the OAuth2 authentication \(p. 26\)](#).

4.1 CONFIGURING THE LDAP AUTHENTICATION

4.1.1 Prerequisites

To set up a link to an LDAP directory, you must check the following:

- If there is a firewall between the Akuiteo server and the directory, this firewall must be configured to let communications go through on the relevant port (389 for example).
- A "technical" account must be created with the following characteristics:
 - The account has read rights to access the whole directory.
 - The account can read all the attributes of a directory's entry.
 - The account is not locked.
 - The password cannot and must not be modified, and never expires.
- The users declared in Akuiteo must have the same login as the one used in the LDAP.

Example

If the user Mary James is declared in the directory as *MJS*, this user's login must also be *MJS* in Akuiteo.

4.1.2 Configuring the Administration console

The information to access an LDAP directory is defined in the Administration console, from the **Security > LDAP** menu.

- 1 From the **LDAP** screen, click on the **New configuration** button at the top right of the screen.

2 In the configuration window, fill in the following fields:

Field	Description
Code	Enter a code to identify the directory. This code must be unique.
Login	Fill in the full login of the technical account, for example <i>CN=LDAPBrowser,OU=Technique,OU=Republique,DC=akuiteo,DC=lan.</i> Tip If you use Active Directory, this login is specified in the properties of the "technical" user > Attribute Editor tab > distinguishedName attribute.
Password	Specify the password associated with the technical account.
Dn Base	Fill in the path to the start of the tree structure, for example <i>OU=Republique,DC=akuiteo,DC=lan.</i> Tip If you use Active Directory, this is specified in the properties at the root of the users tree structure > Attribute Editor tab > dnBase attribute.
URL	Specify the name or IP address of the LDAP server, with the communication port for LDAP accesses (389 by default). The address follows this example: <i>ldap://server:389</i> . You can specify as many URLs as needed, for example in case of a server failure. In this situation, the URL 1 is used in priority. If this URL does not work, the URL 2 is then used, and so on. This switchover is done automatically when the current directory no longer works, without having to restart the Akuiteo server.
By default	If you have configured multiple servers, check this box to define which server to use. If you have only one server configured, you must check this box.
Authentication	Check this box to activate the authentication with the LDAP directory. If the box is not checked, the authentication will be based on another authentication method (if active) or on the database.

3 Click on **Test then save** to test the connection to the LDAP directory using the values specified.

↳ If the connection is made, the directory is added to the Administration console. If the connection cannot be made, an error message is displayed.

To modify the information of a directory, click on  for the relevant directory, make all necessary modifications then click on **Test then save**.

To delete a directory, click on  for the relevant directory then confirm the deletion.

4.2 CONFIGURING THE AZURE AD AUTHENTICATION

Important

Akuiteo does not support the multi-factor authentication (MFA), whether on the Azure or the Office 365 side.

Note

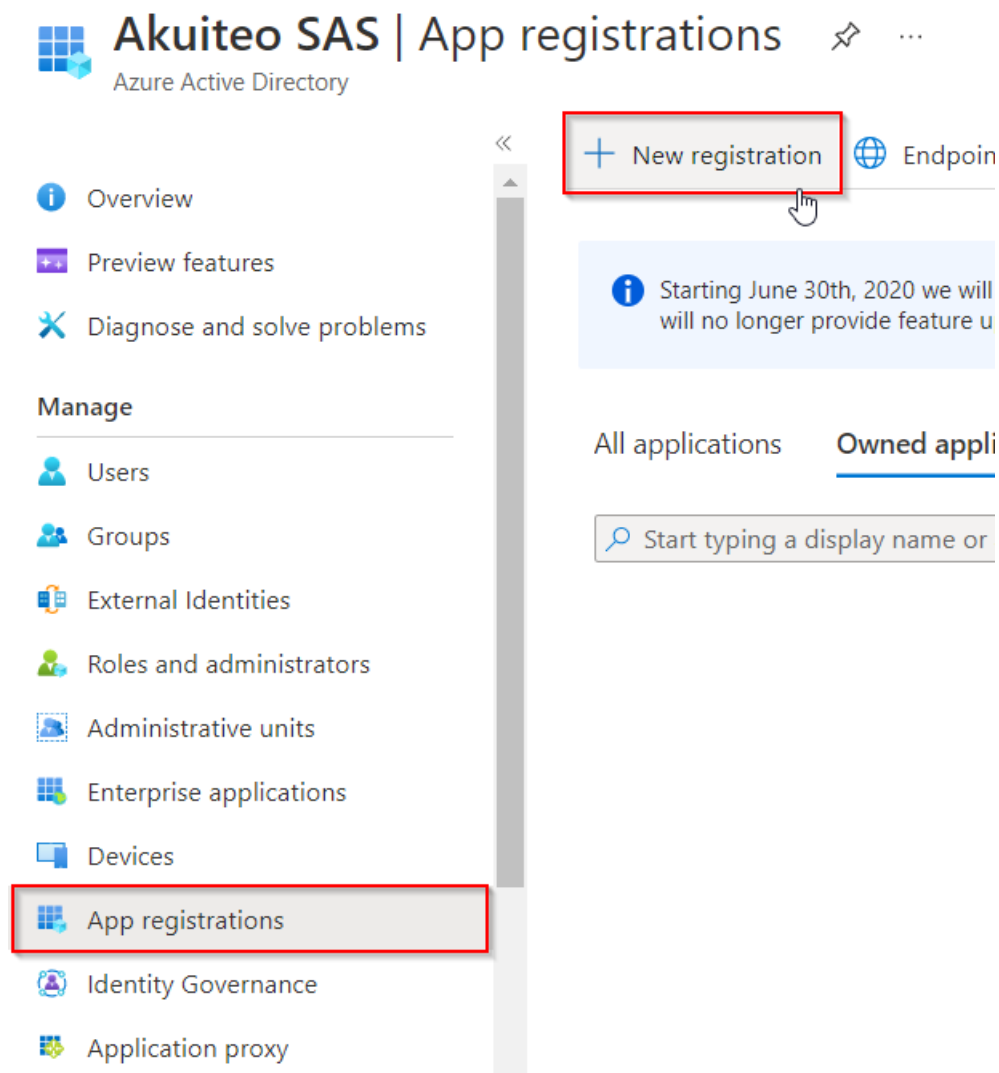
The authentication between Akuiteo and Azure AD uses an email address as the login. This address must be set up correctly in Akuiteo so that the user can log in successfully.

4.2.1 Accessing the Azure portal

- 1 In a web browser, enter the following address <https://portal.azure.com/> and log in as an administrator.
- 2 In the home page, click on the **View** button in the **Manage Azure Active Directory** section.

4.2.2 Registering Akuiteo in the Azure AD's directory

- 1 Click on **App registrations** from the left menu, then click on **New registration**.



- 2 Give a **Name** to this new registration (*Akuiteo* for example) and leave the **Accounts in this organizational directory only (XXX only - Single tenant)** option checked. Click on **Register**.

↳ The application page is displayed with the following information:

- **Application (client) ID:** corresponds to the Client ID in Akuiteo
- **Directory (tenant) ID:** corresponds to the Tenant ID in Akuiteo
- **Object ID:** corresponds to the Application ID in Akuiteo

- 3 Hover over each field then click on the icon that enables you to copy the information to the clipboard. Keep this information in a separate document.

^ Essentials

Display name : [Akuiteo](#)

Application (client) ID : d4e4d823-a15b-4702-aec7-6beb94095b32

Object ID : f6836bd3-4e58-4305-8924-34f9908a9ba3

Directory (tenant) ID : fe36d35c-1016-45f5-ae00-5c283df33f73

Supported account types : [My organization only](#)

Copy to clipboard

4.2.3 Creating a "client secret" to identify the Akuiteo server

- 1 Click on **Certificates & secrets** from the left menu, then click on **New client secret**.

Authentication Certificates (0) **Client secrets (0)** Federated

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

A secret string that the application uses to prove

+ New client secret

Description

No client secrets have been created for this application

- 2 Enter a **Description** (*Akuiteo Secret* for example) then select an expiration date for the key from the **Expires** field, depending on your security policy. Click on **Add**.

Important

When the expiration date is reached, you must create a new "client secret".

- 3 Hover over the line of this "client secret" then click on the button that enables you to copy the information to the clipboard. Keep this information in a separate document.

4.2.4 Allowing the Akuiteo application

From the **API permissions** menu, click on the **Microsoft Graph** API and make sure the Akuiteo application has a **Granted for ...** status. If not, click on **Grant admin consent for XXX**.

- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Akuiteo SAS

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	<div> Granted for Akuiteo SAS ... </div>

To view and manage permissions and user consent, try [Enterprise applications](#).

Note

If this permission is not given, each user will have to grant consent from the Azure portal to be able to connect to Akuiteo.


4.2.5 Configuring the Administration console

The Azure AD directories are defined in the Administration console, from the **Security > Azure AD** menu.

- From the **Azure AD** screen, click on the **New configuration** button at the top right of the screen.
- In the configuration window, fill in the following fields:

Field	Description
Code	Enter a code to identify the directory. This code must be unique.
Tenant Id	Enter the value specified in the Directory (tenant) ID field (in the Azure portal).
Client Id	Enter the value specified in the Application (client) ID field (in the Azure portal).
Client Secret	Enter the value of the client secret (in the Azure portal).
Application Id	Enter the value specified in the Object ID field (in the Azure portal).
Authentication	<p>Check this box to activate the Azure AD authentication.</p> <p>If the box is not checked, the authentication will be based on another authentication method (if active) or on the database.</p>

- Click on **Create**.

 The directory is added to the Administration console.
- Restart the server to take into account the Azure AD directory.

To modify the information of a directory, click on  for the relevant directory, make all necessary modifications then click on **Update**.

To delete a directory, click on  for the relevant directory then confirm the deletion.

4.3 CONFIGURING THE SAML AUTHENTICATION

The SAML (Security Assertion Markup Language) authentication is an open standard that makes it possible to use a single authentication on an identification portal for various applications.

Within the SAML protocol, there are two distinct entities:

- IdP (Identity Provider): The identities manager, that manages authentication and guarantees the authenticity of a person and of the information linked to that person. The following providers are among the most well-known: Microsoft ADFS (via Active Directory), Azure AD, Okta and Auth0.
- SP (Service Provider): The service provider that delegates the authentication to the IdP. This is the Akuiteo server.

Note

The SAML protocol provides two types of operations: the Authentication and the Provisioning. The Provisioning, which is used to create and feed an unknown user, is not handled by Akuiteo.

4.3.1 Prerequisites

Important

The Web Portal and the Customer Portal can never replace the role of SP. You must have access to the Akuiteo server.

As the SP is the Akuiteo server, the user must have access to the following addresses:

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

The user code must be the same as the user's email address.

4.3.2 Preparing the configuration

Creating a certificate store

Note

This step is not required for SaaS customers.

The Akuiteo server must have a certificate file in the .jks format in order to encrypt the exchanges with the IdP. To do this, we use Java Keytool to create a self-signed certificate.

1 On the Akuiteo server, run the following command line:

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

- 2 Fill in the main information of the certificate and make sure to keep the file's password. The following is an example:

```
What is your first and last name?
[Unknown]: Akuiteo
What is the name of your organizational unit?
[Unknown]: IT
What is the name of your organization?
[Unknown]: Akuiteo
What is the name of your City or Locality?
[Unknown]: Lyon
What is the name of your State or Province?
[Unknown]: Rhône
What is the two-letter country code for this unit?
[Unknown]: FR
Is CN=Akuiteo, OU=IT, O=Akuiteo, L=Lyon, ST=Rhône, C=FR correct?
[no]: yes

Enter key password for <saml>
      (press Enter if same as keystore password):
Enter the new password again:

Warning:
The JKS key file uses a proprietary format. It is recommended to migrate to PKCS12 which is
an industry standard format using "keytool -importkeystore -srckeystore saml.jks -
destkeystore saml.jks -deststoretype pkcs12".
```

↳ A saml.jks file is generated. This file will then be used for configuring Akuiteo.

Modifying the Tomcat configuration

- 1 From the Tomcat installation directory of the Akuiteo server, go to **conf**.
- 2 Open the **context.xml** configuration file with a text editor.
- 3 Remove the comment on the <Manager ... /> tag as follows:

```
<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 Restart the Tomcat server to take the modification into account.

Specifying the external URL of the Akuiteo server

When there is a SAML connection ongoing, the Web Portal and Customer Portal redirect to the Akuiteo server in order to initiate the SAML connection. Therefore, the external / public address of the Akuiteo server must be known to the portals.

To do this, two solutions are available:

- Add a configuration item to each portal.
- In the **context.xml** configuration file, add:

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

Limiting the SAML authentication to specific email domains

When the SAML authentication is active, any email login is redirected by default to the IdP in order to be authenticated.

If you want to limit this authentication to specific email domains, add the `saml.domains` parameter (which is linked to the business server) in the **context.xml** configuration file. This parameter enables you to specify:

- either a single domain,
- or a list of domains, separated by a comma (,).

For example:

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

Aligning the JWT secret between the web portals and the Akuiteo server

If the Akuiteo server and the web portals are hosted on separate Tomcat instances, you must "align" the JWT secret, that is to say make sure this secret is the same between all the instances. This secret is used for encrypting employees' login between the various Akuiteo servers. A secret of 63 alphanumeric characters is needed only.

Tip

To generate the JWT secret, you can use a generator (for example <https://www.grc.com/passwords.htm>).

Specify the secret in the JVM parameters of each Tomcat by adding:

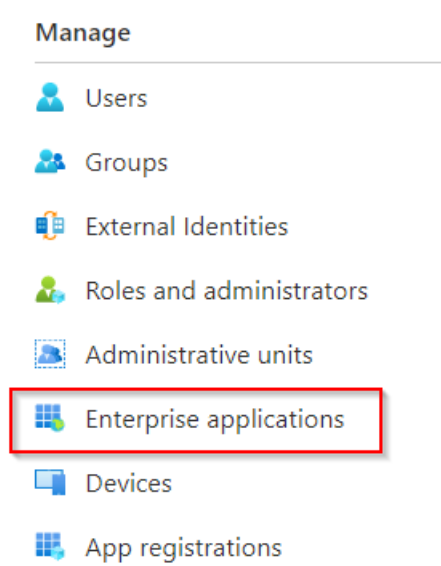
```
-Djwt.secret=iUFmfacoxwH4dzGzd2UxcNsvuebt8rI0wupyN371EREB0uP02x2xzPZuRFjDn0W
```

4.3.3 Creating a SAML application

Note

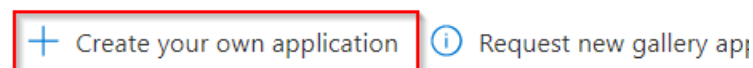
In most cases, the configuration is done with Azure AD. The following process describes how to create a SAML application from the Azure AD portal, but any other identity provider can be used.

- 1 In a web browser, enter the following address <https://portal.azure.com/> and log in as an administrator. In the home page, click on the **View** button in the **Manage Azure Active Directory** section.
- 2 Click on **Enterprise applications** from the left menu, then click on **New application** from the header of the application page.



- 3 Then, click on **Create your own application**.

Browse Azure AD Gallery ...



The Azure AD App Gallery is a catalog of thousands of apps that users more securely to their apps. Browse or create your own ap

- 4 Give an **Input name** to this new application (*Akuiteo-Production* for example) and leave the **Integrate any other application you don't find in the gallery (Non-gallery)** option checked. Then, click on **Create**.
- 5 On the new application's page, select the **2. Set up single sign on** block then select the **SAML** block.
- 6 In the authentication configuration page, fill in the required fields:

- **Identifier (Entity ID)** - URL of your Akuiteo server, for example:
https://akuiteo.myakuiteo.com/akuiteo
- **Reply URL** - URL for the SAML connection based on the previous URL (with the /saml/SSO suffix), for example: *https://akuiteo.myakuiteo.com/akuiteo/saml/SSO*

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Akuiteo-Production.

1

Basic SAML Configuration

Identifier (Entity ID)

Required

Reply URL (Assertion Consumer Service URL)

Required

Sign on URL

Optional

Relay State (Optional)

Optional

Logout Url (Optional)

Optional

Edit

2

Attributes & Claims

⚠ Fill out required fields in Step 1

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

4.3.4 Configuring the Administration console

On Akuiteo's side, the information to configure SAML is defined in the Administration console, from the **Security > SAML** menu.

- 1 From the **SAML configurations** screen, click on the **New configuration** button at the top right of the screen.
- 2 In the configuration window, fill in the following fields:

Field	Description
Code	Enter a code to identify the configuration. This code must be unique.
Active configuration	Check this box to activate the SAML authentication. If the box is not checked, the authentication will be based on another authentication method (if active) or on the database.
IDP	Fill in the IdP's identifier field. If you use Active Directory, this is the Azure AD Identifier .
Audience	Fill in the application ID for the IdP and the public URL.

Field	Description
	If you use Active Directory, this is the Identifier (Entity ID) .
MetaLocation	Fill in the location of the metadata file (URL or local file). If you use Active Directory, this is the URL of the federation metadata file.
KeyAlias	Fill in the alias of the certificate file (.jks).
KeyPwd	Fill in the password of the certificate file (.jks).
KeyLocation	Fill in the location of the certificate file (.jks).

Note

For the MetaLocation and KeyLocation files, the protocol must be specified in the header. If a file is stored locally, add **file:/** at the beginning of the path.

3 Click on **Save**.

↳ If the connection is made, the configuration is added to the Administration console. If the connection cannot be made, an error message is displayed.

4 Restart the server to take the configuration into account.

To modify a configuration, click on  for the relevant line, make all necessary modifications then click on **Update**.

To delete a configuration, click on  for the relevant line then confirm the deletion.

4.4 CONFIGURING THE OAUTH2 AUTHENTICATION

The Oauth2 authentication is only used by Akuiteo for the APIs. This authentication is used to identify the different clients (that is to say the third-party applications) that want to access a resource.

The information to configure Oauth2 is defined in the Administration console, from the **Security > Oauth2** menu.

1 From the **Authorized clients** screen, click on the **New client** button at the top right of the screen.


2 In the configuration window, fill in the following fields:

Field	Description
Client ID	Fill in the Client ID used for the Oauth authentication.
Duration (s)	Fill in the validity duration of the access token, in seconds.
Refresh	The refresh token is used to request a new access token without having to enter the login

Field	Description
duration (s)	information again. Fill in the validity duration of this refresh token, in seconds, that is to say the time during which the refresh token can be used to request a new access token.
Scope	Fill in read_write . Since authorizations are based on DMFs, you can give access to the read_write scope to read, modify and delete resources.

3 Click on **Create**.

↳ The client is added to the Administration console. Akuiteo provides a Client **Secret** associated with this new client, to be used when making calls to APIs.

To modify a client, click on  for the relevant line, make all necessary modifications then click on **Update**.

To delete a client, click on  for the relevant line then confirm the deletion.

Reference

For more information about Akuiteo's APIs, refer to the [API Documentation](#).