Strapi credentials

# Strapi credentials#

You can use these credentials to authenticate the following nodes:

• Strapi

## Prerequisites#

Create a Strapi admin account with:

• Access to an existing Strapi project.

• At least one collection type within that project.

• Published data within that collection type.

Refer to the Strapi developer Quick Start Guide for more information.

## Supported authentication methods#

• API user account: Requires a user account with appropriate content permissions.

• API token: Requires an admin account.

## Related resources#

Refer to Strapi's documentation for more information about the service.

## Using API user account#

To configure this credential, you'll need:

• A user Email: Must be for a user account, not an admin account. Refer to the more detailed instructions below.

• A user Password: Must be for a user account, not an admin account. Refer to the more detailed instructions below.

• The URL: Use the public URL of your Strapi server, defined in ./config/server.js as the url parameter. Strapi recommends using an absolute URL.  
For Strapi Cloud projects, use the URL of your Cloud project, for example: https://my-strapi-project-name.strapiapp.com

./config/server.js

url

• For Strapi Cloud projects, use the URL of your Cloud project, for example: https://my-strapi-project-name.strapiapp.com

https://my-strapi-project-name.strapiapp.com

• The API Version: Select the version of the API you want your calls to use. Options include:  
Version 3  
Version 4

• Version 3

• Version 4

In Strapi, the configuration involves two steps:

• Configure a role.

• Create a user account.

Refer to the more detailed instructions below for each step.

### Configure a role#

For API access, use the Users & Permissions Plugin in Settings > Users & Permissions Plugin.

Refer to Configuring Users & Permissions Plugin for more information on the plugin. Refer to Configuring end-user roles for more information on roles.

For the n8n credential, the user must have a role that grants them API permissions on the collection type. For the role, you can either:

• Update the default Authenticated role to include the permissions and assign the user to that role. Refer to Configuring role's permissions for more information.

• Create a new role to include the permissions and assign the user to that role. Refer to Creating a new role for more information.

For either option, once you open the role:

• Go to the Permissions section.

• Open the section for the relevant collection type.

• Select the permissions for the collection type that the role should have. Options include:  
create (POST)  
find and findone (GET)  
update (PUT)  
delete (DELETE)

• create (POST)

create

• find and findone (GET)

find

findone

• update (PUT)

update

• delete (DELETE)

delete

• Repeat for all relevant collection types.

• Save the role.

Refer to Endpoints for more information on the permission options.

### Create a user account#

Now that you have an appropriate role, create an end-user account and assign the role to it:

• Go to Content Manager > Collection Types > User.

• Select Add new entry.

• Fill in the user details. The n8n credential requires these fields, though your Strapi project may have more custom required fields:  
Username: Required for all Strapi users.  
Email: Enter in Strapi and use as the Email in the n8n credential.  
Password: Enter in Strapi and use as the Password in the n8n credential.  
Role: Select the role you set up in the previous step.

• Username: Required for all Strapi users.

• Email: Enter in Strapi and use as the Email in the n8n credential.

• Password: Enter in Strapi and use as the Password in the n8n credential.

• Role: Select the role you set up in the previous step.

Refer to Managing end-user accounts for more information.

## Using API token#

To configure this credential, you'll need:

• An API Token: Create an API token from Settings > Global Settings > API Tokens. Refer to Strapi's Creating a new API token documentation for more details and information on regenerating API tokens.  
  
API tokens permission  
  
If you don't see the API tokens option in Global settings, your account doesn't have the API tokens > Read permission.

An API Token: Create an API token from Settings > Global Settings > API Tokens. Refer to Strapi's Creating a new API token documentation for more details and information on regenerating API tokens.

API tokens permission

If you don't see the API tokens option in Global settings, your account doesn't have the API tokens > Read permission.

• The URL: Use the public URL of your Strapi server, defined in ./config/server.js as the url parameter. Strapi recommends using an absolute URL.  
  
For Strapi Cloud projects, use the URL of your Cloud project, for example: https://my-strapi-project-name.strapiapp.com

The URL: Use the public URL of your Strapi server, defined in ./config/server.js as the url parameter. Strapi recommends using an absolute URL.

./config/server.js

url

• For Strapi Cloud projects, use the URL of your Cloud project, for example: https://my-strapi-project-name.strapiapp.com

https://my-strapi-project-name.strapiapp.com

• The API Version: Select the version of the API you want your calls to use. Options include:  
Version 3  
Version 4

• Version 3

• Version 4