

For a structure like this where we have distinct authorisation APIs:

auth Overview

The **Auth** API allows users to Login and Logout of the server.

POST /auth/login Validate credentials with the server

POST /auth/logout Remove the server session

The **Employee** API exposes information from the **People** data stored within TRIRIGA. Employee data is represented by TRIRIGA as a collection of records. Some uses for the **Employee** API.

- retrieve the record of a member of staff to check their assigned location.
- align Employee data with an external system so that when a record is created in TRIRIGA by an external system the correct information is assigned to the record.

POST /1.0/employees Create a Employee record

GET /1.0/employees Get any Employee record(s)

Returns all of the **Employee** records. It is recommended to use a query when calling this path.

Security options for login API:

Available authorizations

basicAuth (http, Basic) ←

Basic Authentication to Authorise Requests

Username:

Password:

ApiKeyAuth (apiKey) ←

API Key for mkauth

Name: X-EXPCONNECT-TOKEN

In: header

Value:

Security option for the resource APIs:

Available authorizations

session (apiKey) ←

JSESSION from mkauth

Name: JSESSIONID

In: cookie

Value:

As you can see, we are able to define specific security options on the API path level.

Currently, the connector kit will allow both the basic and API key-based authentication methods, however, these methods are applied globally. We would like to have the capability to support specific connections for specific API paths. This option is supported in OAS 3.0.3 and OAS 3.1 and supported by swagger client.

Connection properties

Basic **API key**

Complete the following fields to configure the form that will be used to connect to the application.

Display name	Property	Required	
Api Key	JSESSIONID	<input type="checkbox"/>	

Description (optional)

Location

Cookie

Display name	Property	Required	
Api Key	X-EXPCONNECT-TOKEN	<input type="checkbox"/>	

Description (optional)

Supported authorization types

- Basic
- Bearer token
- API key
- OAuth2 authorization code
- OAuth2 implicit
- OAuth2 password
- OAuth2 client