June 11, 2020

Automation Anywhere Version A2019

Legal Notices

Examples and graphics are provided only as reference information and might not match your site.

Content

Authentication API overview

Use the Authentication API to generate, refresh, and manage JSON Web Tokens (JWT) that are required for authorization in all Enterprise Control Room APIs.

You can view the Authentication API in the Community Edition.
Note: APIs can be viewed in the Community Edition, but API functionality is limited. You need a licensed Enterprise A2019 Edition to access the full functionality of the APIs.
The JWT is a text string with 703 characters.

```
{
  "token": "eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiIxIiwiY2xpZW50VHlwZSI6IldFQiIsImxpY2
Vuc2VzIjpbXSwiYW5hbHl0aWNzTGljZW5zZXNQdXJjaGFzZWQiOnsiQW5hbHl0aWNzQ2xpZW50Ijp0c
nVlLCJBbmFseXRpY3NBUEkiOnRydWV9LCJpYXQiOjE1NzMxMDc4NzMsImV4cCI6MTU3MzEwOTA3Mywi
aXNzIjoiQXV0b21hdGlvbkFueXdoZXJlIiwibmFub1RpbWUiOjM2NTc1NjI0OTQ2MzE2MDAsImNzcmZ
Ub2tlbiI6ImNiZjgwZWNkZmU5YmUwYzViOGI2MDk3NmU0ZTI2MTNiIn0.rGYxbS5kKUTxtZhYtRSXpm
IHwbf3IwLBIKDEA7odG5uGVAjD55Tv05bYdARx_3-tl1CBg_cDGbwj5FvaBt9u5xKu5W5j3Nur6x3PF
62NeB3ZIdxiUPaFBU0Br84mPJMD4_EpwBfbeSVOMH6ngiLtJYhIOtJa0kp4pAAm3mvkuOUELtH8lf3p
Qf-2Ose2fUAaebDkqiH13SUF1TONAjUQv6Ef_uY0wgq9SjZwKHg9SKUhX3S8PXAJne_ih2QnN8nUE1S
XGlkC04eoIvyWpFkM963XEjptc2uvwtVn42MdA4Nd1opD5yijEl9VM92Fe1sPb6_T5-oV-U1Iw0JHiX
2-Ug",  . . .
}
```

auth

POST `http://<your_control_room_url>/v1/authentication`

Body parameters:

```
{
  "username": "string",
  "password": "string",
  "apiKey": "string"
}
```

Make a post request to generate a JWT.

- The `username` of the Automation Anywhere user.
- The `password` of the Automation Anywhere user.
- The `apiKey` is required to configure Single Sign On (SSO). It can also be used in place of a password for users that are assigned to the API key generation role.

- A JWT is required in the header of other Enterprise Control Room APIs.
- Authentication tokens have a default timeout of 20 minutes.

Not all parameters are required to generate an authentication token. Go to the examples listed here for detailed information.

- Authenticate with username and password
- Authenticate with username and apiKey

Note:

Simple and Protected Negotiation GSSAPI Mechanism (SPNEGO)

You can use SPNEGO, pronounced "spenay-go," when your Enterprise Control Room is configured properly with the following authentication features:

- Active Directory (AD) mode of authentication
- AD is Kerberos enabled

In an Enterprise Control Room with SPNEGO properly configured, users do not need to enter a username and password to generate a JWT.

SPNEGO Authentication API URL example:`https://<your_control_room_url/v1/authentication/SPNEGO`

GET `http://<your_control_room_url>/v1/authentication/token/{token}`

URL parameter:
The token you are validating.
Note: The token is passed as a parameter in the URL. There are no parameters for the request body.

Read Validate an authentication token for task details.

POST `http://<your_control_room_url>/v1/authentication/token`

Body parameter:
A refresh token allows you to get a new token without the need to collect and authenticate credentials every time a token expires.

```
{
  "token": "string"
}
```

Click Refresh an authentication token for a detailed example of this API.

POST `http://<your_control_room_url>/v1/authentication/logout`

Header parameter:
Immediately expires the token that you add to the header of the request.

```
POST 'http://<your_control_room_url>/v1/authentication/logout'
-H 'X-Authorization: <access_token>
```

Click Immediately logout (expire) an authentication token for a detailed example of this API.

POST `http://<your_control_room_url>/v1/authentication/app/login`

The `.../atuhenticataion/app/login` API is a service to service authentication API used by Automation Anywhere internally supported applications. This API is not supported for use by external users.