

Creating a Session Token

Last Modified on 05/28/2024 10:09 am EDT

Overview

Session tokens are required to authenticate an endpoint in order to receive the desired payload. you will receive a 403-authentication error, if an endpoint is not authenticated.

()

Note:

API Keys are the recommended method for endpoint authentication. For more information, refer to the **Create an API Key** article.

User Account Requirements

The user used to login must have Administrator permission to access Swagger Docs.

Related Information/Setup

Please refer to the Locating an Org's ID article for further information on locating your org ID.

Navigation

1. From the *Home* screen, click the **System** icon.



System Icon

2. From the *Admin Overview* screen, click the **Swagger Docs** tile under the **Tools** section.



		Q Search		00	0	\$ \$	2	
Admin Overview	~							
Tools			Communication	s				
?	.⊥		@		S			
Swagger Docs	Data Import	Logo Upload	Email Settings		Languages			
Data Audit Trail	User Audit Trail	Data Audit Archive Export	Email Templates	Portal Settings	×			
Image Upload	Document Management							

Swagger Docs Tile

3. From the *Admin: Swagger* screen, enter authenticate in the **Search** field.

	000	\$? 2				
Tools ~	Swagger Docs	Data Import	Logo Upload	Data Management Audit Trail		
Admin: Help						
Swagger API Documenta	ation					
Swagger provides documentation for	the various API servi	es available.				
Authenticate						
authenticate						~

Search Field

4. Click the **Authenticate** endpoint.

Creating a Session Token

1. From under the Authenticate endpoint, click POST /user/authenticate.



	(Q Search	000	\$ \$ \$
Tools	Swagger Docs Data Import Logo Upload Data Management Audit Trail		_
	authenticate		^
	GET /user/authenticate renew token		\checkmark
	POST /user/authenticate login with credentials		\sim
	POST /user/authenticate/logout logout		\sim
	POST /user/authenticate/productboard Get token product board portal		\sim
	POST /user/authenticate/qrveyComposerToken Get Qrvey composer token		\sim
	POST /user/authenticate/strategy check login strategy based on email		\sim
			-

POST/user/authenticate

2. Click the **Example Value** box to populate the template in the **body** text box.

		⊕ (c	Search			000	ණ	?	
	~	Swagger Docs	Data Import	Logo Upload	Data Management Audit Trail				
POST	/user/authent	ticate login with cre	edentials					^	1
Parame	ters						Cancel		
Name	Description								
body	Edit Value Model								
(body)	0								
								4	
	Click to Populate	Example							
	"email": " "password" "selectedO	'string", ': "string",)rg": 0.							
	"client": "mfaTokenC }	"core-client", code": null							
	Cancel								

Example Value

- Enter your login credentials (email and password) between the quotation marks (e.g., "23145") in the request body.
- 4. Enter the org ID (selectedOrg), Org IDs can be obtained using your browser's dev tools. For further information, see the Locating an Org's ID article.



		⊕ (Q	Search			000	\$?	Ω	1
Tools	~	Swagger Docs	Data Import	Logo Upload	Data Management Audit Trail					
	POST /user/authenti	icate login with cred	lentials					^		
	Parameters						Cancel]		
	Name Description									
	body object (body) Edit Value Model { "email": "Ent "passand": " "elected0" "efalote0Code }	er your Email", Enter your password : Enter the org ID, re-client", ": null	,					4		*

Request Body

- 5. Click the **Execute** button to return one of the following responses:
 - **401 Unauthorized:** The login credentials are incorrect.
 - 404 Not Found: The user is not an active member of any orgs.
 - 200 Success: The user was successfully authenticated.

	⊕ (Q Search							?	Ω	-
Tools	~	Swagger Docs	Data Import	Logo Upload	Data Management Audit Trail					
	Click to Populate { "email": " "password" "selected0 "client": "mfaTokenC } Cancel	Example string", : "string", rg": 0, "core-client", ode": null								
	Parameter conten	on v		Execute						

Execute Button

5. If successful, copy the bearer token to your clipboard. This token is valid for 15 minutes and must be entered in the authorization header of each request.