1.0 Auth APIs

WAS THIS PAGE HELPFUL? Leave Feedback

1.0 Auth APIs

since: 7.0.2

1.1 Login

Authenticates an application, creating an SSO session for the given application. The Login API authenticates an application using three post parameters: user, password and app_name. All of these post parameters are required. Authentication is achieved by calling this API with encoded and/or encrypted credentials in the user and password parameters. The user must always be Base64 encoded. If security encryption is enabled, the encrypted password should be passed without additional encoding; otherwise, unencrypted passwords must be Base64 encoded. If successful, login returns a simple string: an access token. This token must then be passed to all subsequent Rest API calls in the *GWOS-API-TOKEN* HTTP header.

Login can return the follow HTTP Response Codes:

200 - Success
400 - Bad Request - if a parameter is missing or badly formed
401 - Unauthorized - failed to login
500 - General server failure

1.1.1 Method: POST

POST /api/auth/login

1.1.2 HTTP Headers

Header	Valid Values	Required
Accept	text/plain	no
Content-Type	application/x-www-form-urlencoded	no

1.1.3 HTTP Post Parameters

Field	Description	Required
user	Base64 encoded user name	yes
password	encrypted or Base64 encoded password	yes
gwos-app-name	identifies your application name	yes

Post data example:

user=d3N1c2Vy&password=d3N1c2Vy&gwos-app-name=cloudhub

1.2 Logout

Logout will end the SSO session for an application. Logout accepts two required post parameters: gwos_api_token, and app_name. If successful, logout returns an HTTP Status Code of 200. Note that the token may already be expired. In this case, the status code will be 404 Not Found, which can effectively be treated the same way as 200.

Logout can return the follow HTTP Response Codes:

200 - Success
400 - Bad Request - if a parameter is missing or badly formed
404 - Token not found, can be treated like 200 as the token has already expired
500 - General server failure

1.2.1 Method: POST

POST /api/auth/logout

1.2.2 HTTP Headers

Header	Valid Values	Required
Accept	text/plain	no
Content-Type	application/x-www-form-urlencoded	no

1.2.3 HTTP Post Parameters

Field	Description	Required
gwos-api-token	The token returned from login	yes
gwos-app-name	identifies your application name	yes

Post data example:

gwos-api-token=392393939239&gwos-app-name=cloudhub

1.3 Validate Token

Validatetoken will validate the provided token for an application. Validatetoken accepts two required post parameters: gwos_api_token, and app_name. If successful, Validatetoken returns a simple string: 'true' or 'false' indicating whether or not the provided token is valid to use.

Validatetoken can return the follow HTTP Response Codes:

200 - Success
400 - Bad Request - if a parameter is missing or badly formed
500 - General server failure

1.3.1 Method: POST

POST /api/auth/validatetoken

1.2.2 HTTP Headers

Header	Valid Values	Required
Accept	text/plain	no
Content-Type	application/x-www-form-urlencoded	no

1.2.3 HTTP Post Parameters

Field	Description	Required
gwos-api-token	The token returned from login	yes
gwos-app-name	identifies your application name	yes

Post data example:

gwos-api-token=392393939239&gwos-app-name=cloudhub