



OpenShift Container Platform 4.20

OAuth APIs

Reference guide for OAuth APIs

OpenShift Container Platform 4.20 OAuth APIs

Reference guide for Oauth APIs

Legal Notice

Copyright © 2025 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This document describes the OpenShift Container Platform OAuth API objects and their detailed specifications.

Table of Contents

CHAPTER 1. OAUTH APIS	3
1.1. OAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]	3
1.2. OAUTHAUTHORIZETOKEN [OAUTH.OPENSIFT.IO/V1]	3
1.3. OAUTHCLIENTAUTHORIZATION [OAUTH.OPENSIFT.IO/V1]	3
1.4. OAUTHCLIENT [OAUTH.OPENSIFT.IO/V1]	3
1.5. USEROAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]	3
CHAPTER 2. OAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]	5
2.1. SPECIFICATION	5
2.2. API ENDPOINTS	6
2.2.1. /apis/oauth.openshift.io/v1/oauthaccessstokens	7
2.2.2. /apis/oauth.openshift.io/v1/watch/oauthaccessstokens	9
2.2.3. /apis/oauth.openshift.io/v1/oauthaccessstokens/{name}	9
2.2.4. /apis/oauth.openshift.io/v1/watch/oauthaccessstokens/{name}	12
CHAPTER 3. OAUTHAUTHORIZETOKEN [OAUTH.OPENSIFT.IO/V1]	14
3.1. SPECIFICATION	14
3.2. API ENDPOINTS	15
3.2.1. /apis/oauth.openshift.io/v1/oauthauthorizetokens	16
3.2.2. /apis/oauth.openshift.io/v1/watch/oauthauthorizetokens	18
3.2.3. /apis/oauth.openshift.io/v1/oauthauthorizetokens/{name}	18
3.2.4. /apis/oauth.openshift.io/v1/watch/oauthauthorizetokens/{name}	21
CHAPTER 4. OAUTHCLIENTAUTHORIZATION [OAUTH.OPENSIFT.IO/V1]	23
4.1. SPECIFICATION	23
4.2. API ENDPOINTS	24
4.2.1. /apis/oauth.openshift.io/v1/oauthclientauthorizations	24
4.2.2. /apis/oauth.openshift.io/v1/watch/oauthclientauthorizations	26
4.2.3. /apis/oauth.openshift.io/v1/oauthclientauthorizations/{name}	27
4.2.4. /apis/oauth.openshift.io/v1/watch/oauthclientauthorizations/{name}	30
CHAPTER 5. OAUTHCLIENT [OAUTH.OPENSIFT.IO/V1]	31
5.1. SPECIFICATION	31
5.1.1. .scopeRestrictions	33
5.1.2. .scopeRestrictions[]	33
5.1.3. .scopeRestrictions[].clusterRole	33
5.2. API ENDPOINTS	34
5.2.1. /apis/oauth.openshift.io/v1/oauthclients	35
5.2.2. /apis/oauth.openshift.io/v1/watch/oauthclients	37
5.2.3. /apis/oauth.openshift.io/v1/oauthclients/{name}	37
5.2.4. /apis/oauth.openshift.io/v1/watch/oauthclients/{name}	40
CHAPTER 6. USEROAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]	42
6.1. SPECIFICATION	42
6.2. API ENDPOINTS	43
6.2.1. /apis/oauth.openshift.io/v1/useroauthaccessstokens	44
6.2.2. /apis/oauth.openshift.io/v1/watch/useroauthaccessstokens	44
6.2.3. /apis/oauth.openshift.io/v1/useroauthaccessstokens/{name}	44
6.2.4. /apis/oauth.openshift.io/v1/watch/useroauthaccessstokens/{name}	45

CHAPTER 1. OAUTH APIS

1.1. OAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]

Description

OAuthAccessToken describes an OAuth access token. The name of a token must be prefixed with a **sha256~** string, must not contain "/" or "%" characters and must be at least 32 characters long.

The name of the token is constructed from the actual token by sha256-hashing it and using URL-safe unpadded base64-encoding (as described in RFC4648) on the hashed result.

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

1.2. OAUTHAUTHORIZETOKEN [OAUTH.OPENSIFT.IO/V1]

Description

OAuthAuthorizeToken describes an OAuth authorization token

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

1.3. OAUTHCLIENTAUTHORIZATION [OAUTH.OPENSIFT.IO/V1]

Description

OAuthClientAuthorization describes an authorization created by an OAuth client

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

1.4. OAUTHCLIENT [OAUTH.OPENSIFT.IO/V1]

Description

OAuthClient describes an OAuth client

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

1.5. USEROAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]

Description

UserOAuthAccessToken is a virtual resource to mirror OAuthAccessTokens to the user the access token was issued for

Type

object

CHAPTER 2. OAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]

Description

OAuthAccessToken describes an OAuth access token. The name of a token must be prefixed with a **sha256~** string, must not contain "/" or "%" characters and must be at least 32 characters long.

The name of the token is constructed from the actual token by sha256-hashing it and using URL-safe unpadded base64-encoding (as described in RFC4648) on the hashed result.

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

2.1. SPECIFICATION

Property	Type	Description
apiVersion	string	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resources
authorizeToken	string	authorizeToken contains the token that authorized this token
clientName	string	clientName references the client that created this token.
expiresIn	integer	expiresIn is the seconds from CreationTime before this token expires.
inactivityTimeoutSeconds	integer	inactivityTimeoutSeconds is the value in seconds, from the CreationTimestamp, after which this token can no longer be used. The value is automatically incremented when the token is used.

Property	Type	Description
kind	string	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds
metadata	ObjectMeta	metadata is the standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata
redirectURI	string	redirectURI is the redirection associated with the token.
refreshToken	string	refreshToken is the value by which this token can be renewed. Can be blank.
scopes	array (string)	scopes is an array of the requested scopes.
userName	string	userName is the user name associated with this token
userID	string	userID is the unique UID associated with this token

2.2. API ENDPOINTS

The following API endpoints are available:

- **/apis/oauth.openshift.io/v1/oauthaccesstokens**
 - **DELETE**: delete collection of OAuthAccessToken
 - **GET**: list or watch objects of kind OAuthAccessToken
 - **POST**: create an OAuthAccessToken
- **/apis/oauth.openshift.io/v1/watch/oauthaccesstokens**

- **GET**: watch individual changes to a list of OAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead.
- **/apis/oauth.openshift.io/v1/oauthaccesstokens/{name}**
 - **DELETE**: delete an OAuthAccessToken
 - **GET**: read the specified OAuthAccessToken
 - **PATCH**: partially update the specified OAuthAccessToken
 - **PUT**: replace the specified OAuthAccessToken
- **/apis/oauth.openshift.io/v1/watch/oauthaccesstokens/{name}**
 - **GET**: watch changes to an object of kind OAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

2.2.1. /apis/oauth.openshift.io/v1/oauthaccesstokens

HTTP method

DELETE

Description

delete collection of OAuthAccessToken

Table 2.1. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 2.2. HTTP responses

HTTP code	Reponse body
200 - OK	Status schema
401 - Unauthorized	Empty

HTTP method

GET

Description

list or watch objects of kind OAuthAccessToken

Table 2.3. HTTP responses

HTTP code	Response body
200 - OK	OAuthAccessTokenList schema
401 - Unauthorized	Empty

HTTP method**POST****Description**

create an OAuthAccessToken

Table 2.4. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 2.5. Body parameters

Parameter	Type	Description
body	OAuthAccessToken schema	

Table 2.6. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthAccessToken schema
201 - Created	OAuthAccessToken schema
202 - Accepted	OAuthAccessToken schema
401 - Unauthorized	Empty

2.2.2. /apis/oauth.openshift.io/v1/watch/oauthaccesstokens

HTTP method

GET

Description

watch individual changes to a list of OAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead.

Table 2.7. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

2.2.3. /apis/oauth.openshift.io/v1/oauthaccesstokens/{name}

Table 2.8. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthAccessToken

HTTP method

DELETE

Description

delete an OAuthAccessToken

Table 2.9. Query parameters

Parameter	Type	Description
-----------	------	-------------

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 2.10. HTTP responses

HTTP code	Response body
200 - OK	OAuthAccessToken schema
202 - Accepted	OAuthAccessToken schema
401 - Unauthorized	Empty

HTTP method**GET****Description**

read the specified OAuthAccessToken

Table 2.11. HTTP responses

HTTP code	Response body
200 - OK	OAuthAccessToken schema
401 - Unauthorized	Empty

HTTP method**PATCH****Description**

partially update the specified OAuthAccessToken

Table 2.12. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Parameter	Type	Description
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 2.13. HTTP responses

HTTP code	Response body
200 - OK	OAuthAccessToken schema
201 - Created	OAuthAccessToken schema
401 - Unauthorized	Empty

HTTP method**PUT****Description**

replace the specified OAuthAccessToken

Table 2.14. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Parameter	Type	Description
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 2.15. Body parameters

Parameter	Type	Description
body	OAuthAccessToken schema	

Table 2.16. HTTP responses

HTTP code	Response body
200 - OK	OAuthAccessToken schema
201 - Created	OAuthAccessToken schema
401 - Unauthorized	Empty

2.2.4. /apis/oauth.openshift.io/v1/watch/oauthaccesstokens/{name}

Table 2.17. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthAccessToken

HTTP method

GET

Description

watch changes to an object of kind OAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

Table 2.18. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

CHAPTER 3. OAUTHAUTHORIZETOKEN [OAUTH.OPENSIFT.IO/V1]

Description

OAuthAuthorizeToken describes an OAuth authorization token

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

3.1. SPECIFICATION

Property	Type	Description
apiVersion	string	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resources
clientName	string	clientName references the client that created this token.
codeChallenge	string	codeChallenge is the optional code_challenge associated with this authorization code, as described in rfc7636
codeChallengeMethod	string	codeChallengeMethod is the optional code_challenge_method associated with this authorization code, as described in rfc7636
expiresIn	integer	expiresIn is the seconds from CreationTime before this token expires.

Property	Type	Description
kind	string	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds
metadata	ObjectMeta	metadata is the standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata
redirectURI	string	redirectURI is the redirection associated with the token.
scopes	array (string)	scopes is an array of the requested scopes.
state	string	state data from request
userName	string	userName is the user name associated with this token
userID	string	userID is the unique UID associated with this token. UserID and UserName must both match for this token to be valid.

3.2. API ENDPOINTS

The following API endpoints are available:

- **/apis/oauth.openshift.io/v1/oauthauthorizetokens**
 - **DELETE**: delete collection of OAuthAuthorizeToken
 - **GET**: list or watch objects of kind OAuthAuthorizeToken
 - **POST**: create an OAuthAuthorizeToken
- **/apis/oauth.openshift.io/v1/watch/oauthauthorizetokens**

- **GET**: watch individual changes to a list of OAuthAuthorizeToken. deprecated: use the 'watch' parameter with a list operation instead.
- **/apis/oauth.openshift.io/v1/oauthauthorizetokens/{name}**
 - **DELETE**: delete an OAuthAuthorizeToken
 - **GET**: read the specified OAuthAuthorizeToken
 - **PATCH**: partially update the specified OAuthAuthorizeToken
 - **PUT**: replace the specified OAuthAuthorizeToken
- **/apis/oauth.openshift.io/v1/watch/oauthauthorizetokens/{name}**
 - **GET**: watch changes to an object of kind OAuthAuthorizeToken. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

3.2.1. /apis/oauth.openshift.io/v1/oauthauthorizetokens

HTTP method

DELETE

Description

delete collection of OAuthAuthorizeToken

Table 3.1. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 3.2. HTTP responses

HTTP code	Response body
200 - OK	Status schema
401 - Unauthorized	Empty

HTTP method

GET

Description

list or watch objects of kind OAuthAuthorizeToken

Table 3.3. HTTP responses

HTTP code	Response body
200 - OK	OAuthAuthorizeTokenList schema
401 - Unauthorized	Empty

HTTP method**POST****Description**

create an OAuthAuthorizeToken

Table 3.4. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 3.5. Body parameters

Parameter	Type	Description
body	OAuthAuthorizeToken schema	

Table 3.6. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthAuthorizeToken schema
201 - Created	OAuthAuthorizeToken schema
202 - Accepted	OAuthAuthorizeToken schema
401 - Unauthorized	Empty

3.2.2. /apis/oauth.openshift.io/v1/watch/oauthauthorizetokens

HTTP method

GET

Description

watch individual changes to a list of OAuthAuthorizeToken. deprecated: use the 'watch' parameter with a list operation instead.

Table 3.7. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

3.2.3. /apis/oauth.openshift.io/v1/oauthauthorizetokens/{name}

Table 3.8. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthAuthorizeToken

HTTP method

DELETE

Description

delete an OAuthAuthorizeToken

Table 3.9. Query parameters

Parameter	Type	Description
-----------	------	-------------

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 3.10. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthAuthorizeToken schema
202 - Accepted	OAuthAuthorizeToken schema
401 - Unauthorized	Empty

HTTP method**GET****Description**

read the specified OAuthAuthorizeToken

Table 3.11. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthAuthorizeToken schema
401 - Unauthorized	Empty

HTTP method**PATCH****Description**

partially update the specified OAuthAuthorizeToken

Table 3.12. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Parameter	Type	Description
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 3.13. HTTP responses

HTTP code	Response body
200 - OK	OAuthAuthorizeToken schema
201 - Created	OAuthAuthorizeToken schema
401 - Unauthorized	Empty

HTTP method**PUT****Description**

replace the specified OAuthAuthorizeToken

Table 3.14. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Parameter	Type	Description
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 3.15. Body parameters

Parameter	Type	Description
body	OAuthAuthorizeToken schema	

Table 3.16. HTTP responses

HTTP code	Response body
200 - OK	OAuthAuthorizeToken schema
201 - Created	OAuthAuthorizeToken schema
401 - Unauthorized	Empty

3.2.4. /apis/oauth.openshift.io/v1/watch/oauthauthorizetokens/{name}

Table 3.17. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthAuthorizeToken

HTTP method

GET

Description

watch changes to an object of kind OAuthAuthorizeToken. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

Table 3.18. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

CHAPTER 4. OAUTHCLIENTAUTHORIZATION [OAUTH.OPENSIFT.IO/V1]

Description

OAuthClientAuthorization describes an authorization created by an OAuth client

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

4.1. SPECIFICATION

Property	Type	Description
apiVersion	string	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resources
clientName	string	clientName references the client that created this authorization
kind	string	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds
metadata	ObjectMeta	metadata is the standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata
scopes	array (string)	scopes is an array of the granted scopes.

Property	Type	Description
userName	string	userName is the user name that authorized this client
userID	string	userID is the unique UID associated with this authorization. UserID and UserName must both match for this authorization to be valid.

4.2. API ENDPOINTS

The following API endpoints are available:

- **/apis/oauth.openshift.io/v1/oauthclientauthorizations**
 - **DELETE**: delete collection of OAuthClientAuthorization
 - **GET**: list or watch objects of kind OAuthClientAuthorization
 - **POST**: create an OAuthClientAuthorization
- **/apis/oauth.openshift.io/v1/watch/oauthclientauthorizations**
 - **GET**: watch individual changes to a list of OAuthClientAuthorization. deprecated: use the 'watch' parameter with a list operation instead.
- **/apis/oauth.openshift.io/v1/oauthclientauthorizations/{name}**
 - **DELETE**: delete an OAuthClientAuthorization
 - **GET**: read the specified OAuthClientAuthorization
 - **PATCH**: partially update the specified OAuthClientAuthorization
 - **PUT**: replace the specified OAuthClientAuthorization
- **/apis/oauth.openshift.io/v1/watch/oauthclientauthorizations/{name}**
 - **GET**: watch changes to an object of kind OAuthClientAuthorization. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

4.2.1. /apis/oauth.openshift.io/v1/oauthclientauthorizations

HTTP method

DELETE

Description

delete collection of OAuthClientAuthorization

Table 4.1. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 4.2. HTTP responses

HTTP code	Reponse body
200 - OK	Status schema
401 - Unauthorized	Empty

HTTP method**GET****Description**

list or watch objects of kind OAuthClientAuthorization

Table 4.3. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthClientAuthorizationList schema
401 - Unauthorized	Empty

HTTP method**POST****Description**

create an OAuthClientAuthorization

Table 4.4. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Parameter	Type	Description
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 4.5. Body parameters

Parameter	Type	Description
body	OAuthClientAuthorization schema	

Table 4.6. HTTP responses

HTTP code	Response body
200 - OK	OAuthClientAuthorization schema
201 - Created	OAuthClientAuthorization schema
202 - Accepted	OAuthClientAuthorization schema
401 - Unauthorized	Empty

4.2.2. /apis/oauth.openshift.io/v1/watch/oauthclientauthorizations

HTTP method

GET

Description

watch individual changes to a list of OAuthClientAuthorization. deprecated: use the 'watch' parameter with a list operation instead.

Table 4.7. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

4.2.3. /apis/oauth.openshift.io/v1/oauthclientauthorizations/{name}

Table 4.8. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthClientAuthorization

HTTP method

DELETE

Description

delete an OAuthClientAuthorization

Table 4.9. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 4.10. HTTP responses

HTTP code	Reponse body
200 - OK	Status schema
202 - Accepted	Status schema
401 - Unauthorized	Empty

HTTP method

GET

Description

read the specified OAuthClientAuthorization

Table 4.11. HTTP responses

HTTP code	Response body
200 - OK	OAuthClientAuthorization schema
401 - Unauthorized	Empty

HTTP method

PATCH

Description

partially update the specified OAuthClientAuthorization

Table 4.12. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 4.13. HTTP responses

HTTP code	Response body
200 - OK	OAuthClientAuthorization schema
201 - Created	OAuthClientAuthorization schema

HTTP code	Response body
401 - Unauthorized	Empty

HTTP method**PUT****Description**

replace the specified OAuthClientAuthorization

Table 4.14. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 4.15. Body parameters

Parameter	Type	Description
body	OAuthClientAuthorization schema	

Table 4.16. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthClientAuthorization schema
201 - Created	OAuthClientAuthorization schema
401 - Unauthorized	Empty

4.2.4. /apis/oauth.openshift.io/v1/watch/oauthclientauthorizations/{name}

Table 4.17. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthClientAuthorization

HTTP method

GET

Description

watch changes to an object of kind OAuthClientAuthorization. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

Table 4.18. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

CHAPTER 5. OAUTHCLIENT [OAUTH.OPENSIFT.IO/V1]

Description

OAuthClient describes an OAuth client

Compatibility level 1: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

Type

object

5.1. SPECIFICATION

Property	Type	Description
accessTokenInactivityTimeoutSeconds	integer	accessTokenInactivityTimeoutSeconds overrides the default token inactivity timeout for tokens granted to this client. The value represents the maximum amount of time that can occur between consecutive uses of the token. Tokens become invalid if they are not used within this temporal window. The user will need to acquire a new token to regain access once a token times out. This value needs to be set only if the default set in configuration is not appropriate for this client. Valid values are: - 0: Tokens for this client never time out - X: Tokens time out if there is no activity for X seconds The current minimum allowed value for X is 300 (5 minutes) WARNING: existing tokens' timeout will not be affected (lowered) by changing this value
accessTokenMaxAgeSeconds	integer	accessTokenMaxAgeSeconds overrides the default access token max age for tokens granted to this client. 0 means no expiration.
additionalSecrets	array (string)	additionalSecrets holds other secrets that may be used to identify the client. This is useful for rotation and for service account token validation

Property	Type	Description
apiVersion	string	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resources
grantMethod	string	grantMethod is a required field which determines how to handle grants for this client. Valid grant handling methods are: - auto: always approves grant requests, useful for trusted clients - prompt: prompts the end user for approval of grant requests, useful for third-party clients
kind	string	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds
metadata	ObjectMeta	metadata is the standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata
redirectURIs	array (string)	redirectURIs is the valid redirection URIs associated with a client
respondWithChallenges	boolean	respondWithChallenges indicates whether the client wants authentication needed responses made in the form of challenges instead of redirects

Property	Type	Description
scopeRestrictions	array	scopeRestrictions describes which scopes this client can request. Each requested scope is checked against each restriction. If any restriction matches, then the scope is allowed. If no restriction matches, then the scope is denied.
scopeRestrictions[]	object	ScopeRestriction describe one restriction on scopes. Exactly one option must be non-nil.
secret	string	secret is the unique secret associated with a client

5.1.1. .scopeRestrictions

Description

scopeRestrictions describes which scopes this client can request. Each requested scope is checked against each restriction. If any restriction matches, then the scope is allowed. If no restriction matches, then the scope is denied.

Type

array

5.1.2. .scopeRestrictions[]

Description

ScopeRestriction describe one restriction on scopes. Exactly one option must be non-nil.

Type

object

Property	Type	Description
clusterRole	object	ClusterRoleScopeRestriction describes restrictions on cluster role scopes
literals	array (string)	ExactValues means the scope has to match a particular set of strings exactly

5.1.3. .scopeRestrictions[].clusterRole

Description

ClusterRoleScopeRestriction describes restrictions on cluster role scopes

Type

object

Required

- **roleNames**
- **namespaces**
- **allowEscalation**

Property	Type	Description
allowEscalation	boolean	allowEscalation indicates whether you can request roles and their escalating resources
namespaces	array (string)	namespaces is the list of namespaces that can be referenced. * means any of them (including *)
roleNames	array (string)	roleNames is the list of cluster roles that can be referenced. * means anything

5.2. API ENDPOINTS

The following API endpoints are available:

- **/apis/oauth.openshift.io/v1/oauthclients**
 - **DELETE**: delete collection of OAuthClient
 - **GET**: list or watch objects of kind OAuthClient
 - **POST**: create an OAuthClient
- **/apis/oauth.openshift.io/v1/watch/oauthclients**
 - **GET**: watch individual changes to a list of OAuthClient. deprecated: use the 'watch' parameter with a list operation instead.
- **/apis/oauth.openshift.io/v1/oauthclients/{name}**
 - **DELETE**: delete an OAuthClient
 - **GET**: read the specified OAuthClient
 - **PATCH**: partially update the specified OAuthClient
 - **PUT**: replace the specified OAuthClient

- **/apis/oauth.openshift.io/v1/watch/oauthclients/{name}**
 - **GET**: watch changes to an object of kind OAuthClient. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

5.2.1. /apis/oauth.openshift.io/v1/oauthclients

HTTP method

DELETE

Description

delete collection of OAuthClient

Table 5.1. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 5.2. HTTP responses

HTTP code	Reponse body
200 - OK	Status schema
401 - Unauthorized	Empty

HTTP method

GET

Description

list or watch objects of kind OAuthClient

Table 5.3. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthClientList schema
401 - Unauthorized	Empty

HTTP method

POST

Description

create an OAuthClient

Table 5.4. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 5.5. Body parameters

Parameter	Type	Description
body	OAuthClient schema	

Table 5.6. HTTP responses

HTTP code	Response body
200 - OK	OAuthClient schema
201 - Created	OAuthClient schema
202 - Accepted	OAuthClient schema
401 - Unauthorized	Empty

5.2.2. /apis/oauth.openshift.io/v1/watch/oauthclients

HTTP method

GET

Description

watch individual changes to a list of OAuthClient. deprecated: use the 'watch' parameter with a list operation instead.

Table 5.7. HTTP responses

HTTP code	Response body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

5.2.3. /apis/oauth.openshift.io/v1/oauthclients/{name}

Table 5.8. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthClient

HTTP method

DELETE

Description

delete an OAuthClient

Table 5.9. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 5.10. HTTP responses

HTTP code	Response body
200 - OK	Status schema
202 - Accepted	Status schema

HTTP code	Reponse body
401 - Unauthorized	Empty

HTTP method**GET****Description**

read the specified OAuthClient

Table 5.11. HTTP responses

HTTP code	Reponse body
200 - OK	OAuthClient schema
401 - Unauthorized	Empty

HTTP method**PATCH****Description**

partially update the specified OAuthClient

Table 5.12. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Parameter	Type	Description
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 5.13. HTTP responses

HTTP code	Response body
200 - OK	OAuthClient schema
201 - Created	OAuthClient schema
401 - Unauthorized	Empty

HTTP method**PUT****Description**

replace the specified OAuthClient

Table 5.14. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Parameter	Type	Description
fieldValidation	string	fieldValidation instructs the server on how to handle objects in the request (POST/PUT/PATCH) containing unknown or duplicate fields. Valid values are: - Ignore: This will ignore any unknown fields that are silently dropped from the object, and will ignore all but the last duplicate field that the decoder encounters. This is the default behavior prior to v1.23. - Warn: This will send a warning via the standard warning response header for each unknown field that is dropped from the object, and for each duplicate field that is encountered. The request will still succeed if there are no other errors, and will only persist the last of any duplicate fields. This is the default in v1.23+ - Strict: This will fail the request with a BadRequest error if any unknown fields would be dropped from the object, or if any duplicate fields are present. The error returned from the server will contain all unknown and duplicate fields encountered.

Table 5.15. Body parameters

Parameter	Type	Description
body	OAuthClient schema	

Table 5.16. HTTP responses

HTTP code	Response body
200 - OK	OAuthClient schema
201 - Created	OAuthClient schema
401 - Unauthorized	Empty

5.2.4. /apis/oauth.openshift.io/v1/watch/oauthclients/{name}

Table 5.17. Global path parameters

Parameter	Type	Description
name	string	name of the OAuthClient

HTTP method

GET

Description

watch changes to an object of kind OAuthClient. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

Table 5.18. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

CHAPTER 6. USEROAUTHACCESSTOKEN [OAUTH.OPENSIFT.IO/V1]

Description

UserOAuthAccessToken is a virtual resource to mirror OAuthAccessTokens to the user the access token was issued for

Type

object

6.1. SPECIFICATION

Property	Type	Description
apiVersion	string	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resources
authorizeToken	string	authorizeToken contains the token that authorized this token
clientName	string	clientName references the client that created this token.
expiresIn	integer	expiresIn is the seconds from CreationTime before this token expires.
inactivityTimeoutSeconds	integer	inactivityTimeoutSeconds is the value in seconds, from the CreationTimestamp, after which this token can no longer be used. The value is automatically incremented when the token is used.

Property	Type	Description
kind	string	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds
metadata	ObjectMeta	metadata is the standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata
redirectURI	string	redirectURI is the redirection associated with the token.
refreshToken	string	refreshToken is the value by which this token can be renewed. Can be blank.
scopes	array (string)	scopes is an array of the requested scopes.
userName	string	userName is the user name associated with this token
userID	string	userID is the unique UID associated with this token

6.2. API ENDPOINTS

The following API endpoints are available:

- **/apis/oauth.openshift.io/v1/useroauthaccesstokens**
 - **GET**: list or watch objects of kind UserOAuthAccessToken
- **/apis/oauth.openshift.io/v1/watch/useroauthaccesstokens**
 - **GET**: watch individual changes to a list of UserOAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead.

- **/apis/oauth.openshift.io/v1/useroauthaccesstokens/{name}**
 - **DELETE**: delete an UserOAuthAccessToken
 - **GET**: read the specified UserOAuthAccessToken
- **/apis/oauth.openshift.io/v1/watch/useroauthaccesstokens/{name}**
 - **GET**: watch changes to an object of kind UserOAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

6.2.1. /apis/oauth.openshift.io/v1/useroauthaccesstokens

HTTP method

GET

Description

list or watch objects of kind UserOAuthAccessToken

Table 6.1. HTTP responses

HTTP code	Reponse body
200 - OK	UserOAuthAccessTokenList schema
401 - Unauthorized	Empty

6.2.2. /apis/oauth.openshift.io/v1/watch/useroauthaccesstokens

HTTP method

GET

Description

watch individual changes to a list of UserOAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead.

Table 6.2. HTTP responses

HTTP code	Reponse body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty

6.2.3. /apis/oauth.openshift.io/v1/useroauthaccesstokens/{name}

Table 6.3. Global path parameters

Parameter	Type	Description
name	string	name of the UserOAuthAccessToken

HTTP method**DELETE****Description**

delete an UserOAuthAccessToken

Table 6.4. Query parameters

Parameter	Type	Description
dryRun	string	When present, indicates that modifications should not be persisted. An invalid or unrecognized dryRun directive will result in an error response and no further processing of the request. Valid values are: - All: all dry run stages will be processed

Table 6.5. HTTP responses

HTTP code	Reponse body
200 - OK	Status schema
202 - Accepted	Status schema
401 - Unauthorized	Empty

HTTP method**GET****Description**

read the specified UserOAuthAccessToken

Table 6.6. HTTP responses

HTTP code	Reponse body
200 - OK	UserOAuthAccessToken schema
401 - Unauthorized	Empty

6.2.4. /apis/oauth.openshift.io/v1/watch/useroauthaccesstokens/{name}**Table 6.7. Global path parameters**

Parameter	Type	Description
name	string	name of the UserOAuthAccessToken

HTTP method

GET

Description

watch changes to an object of kind UserOAuthAccessToken. deprecated: use the 'watch' parameter with a list operation instead, filtered to a single item with the 'fieldSelector' parameter.

Table 6.8. HTTP responses

HTTP code	Response body
200 - OK	WatchEvent schema
401 - Unauthorized	Empty