



View and create OAuth 2.0 configurations

ONTAP 9.14.1 REST API reference

NetApp
May 08, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi/ontap/security_authentication_cluster_oauth2_clients_endpoint_overview.html on May 08, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- View and create OAuth 2.0 configurations 1
 - Security authentication cluster oauth2 clients endpoint overview 1

View and create OAuth 2.0 configurations

Security authentication cluster oauth2 clients endpoint overview

Overview

This API is used to retrieve and configure relevant information pertaining to the OAuth 2.0 configuration in the cluster. The POST request creates the OAuth 2.0 configuration if there is none present. Various responses are shown in the examples below.

Examples

Retrieving the OAuth 2.0 configuration in the cluster

The following output shows the OAuth 2.0 configuration in the cluster.

```
# The API:
/api/security/authentication/cluster/oauth2/clients

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/authentication/cluster/oauth2/clients" -H "accept:
application/hal+json"

# The response:
{
  "records": [
    {
      "name": "auth0"
    }
  ],
  "num_records": 1
}
```

Creating the OAuth 2.0 configuration

The following output shows how to create the OAuth 2.0 configuration in the cluster.

= The API:

/api/security/authentication/cluster/oauth2/clients

= The call:

```
curl -X POST "https://+++<mgmt-  
ip>+++/api/security/authentication/cluster/oauth2/clients?return_records=t  
rue" -H "accept: application/hal+json" -d '{ "name": "name",  
"application": "http", "issuer": "https://examplelab.customer.com",  
"audience": "aud", "client_id": "client_id", "client_secret":  
"client_secret", "introspection": {"endpoint_uri":  
"https://examplelab.customer.com/server/endpoint", "interval": "PT1H" },  
"remote_user_claim": "user_claim", "outgoing_proxy":  
"https://johndoe:somesecret@proxy.example.com:8080",  
"use_local_roles_if_present": false, "use_mutual_tls": "required"  
'+++</mgmt-ip>+++
```

= The response:

```
{  
  "job": {  
    "uuid": "e45b123b-c228-11e8-aa20-0050568e36bb",  
    "_links": {  
      "self": {  
        "href": "/api/cluster/jobs/e45b123b-c228-11e8-aa20-0050568e36bb"  
      }  
    }  
  }  
}  
'''
```

[[IDa556eec8bef52c4938c818000234033e]]

= Retrieve all OAuth 2.0 configurations

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/oauth2/clients`#

Introduced In: 9.14

Retrieves all OAuth 2.0 configurations.

== Related ONTAP commands

* `security oauth2 client show`

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|use_mutual_tls

|string

|query

|False

a|Filter by use_mutual_tls

|introspection.endpoint_uri

|string

|query

|False

a|Filter by introspection.endpoint_uri

|introspection.interval

|string

|query

|False

a|Filter by introspection.interval

|jwks.refresh_interval

|string

|query

|False

a|Filter by jwks.refresh_interval

|jwks.provider_uri

|string

|query

```
|False
a|Filter by jwks.provider_uri

|audience
|string
|query
|False
a|Filter by audience

|application
|string
|query
|False
a|Filter by application

|name
|string
|query
|False
a|Filter by name

|issuer
|string
|query
|False
a|Filter by issuer

|outgoing_proxy
|string
|query
|False
a|Filter by outgoing_proxy

|hashed_client_secret
|string
|query
|False
a|Filter by hashed_client_secret

|use_local_roles_if_present
```

```
|boolean
|query
|False
a|Filter by use_local_roles_if_present
```

```
|client_id
|string
|query
|False
a|Filter by client_id
```

```
|remote_user_claim
|string
|query
|False
a|Filter by remote_user_claim
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.
```

* Default value: 1

```
|return_timeout
|integer
|query
|False
a|The number of seconds to allow the call to execute before returning.
When iterating over a collection, the default is 15 seconds. ONTAP
returns earlier if either max records or the end of the collection is
reached.
```

* Default value: 1

```

* Max value: 120
* Min value: 0

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records.

|records
|array[link:#security_oauth2[security_oauth2]]
a|

|===

```



```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "application": "http",
    "hashed_client_secret": "string",
    "introspection": {
      "endpoint_uri": "https://examplelab.customer.com/token/introspect",
      "interval": "PT1H"
    },
    "issuer": "https://examplelab.customer.com",
    "jwks": {
      "provider_uri": "https://examplelab.customer.com/pf/JWKS",
      "refresh_interval": "PT2H"
    },
    "name": "auth0",
    "outgoing_proxy": "https://johndoe:secretpass@proxy.example.com:8080",
    "use_mutual_tls": "none"
  }
}
====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|====
|Name
```

```

|Type
|Description

|error
|link:#returned_error[returned_error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string

```

```

a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#introspection]
[.api-collapsible-fifth-title]
introspection

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|endpoint_uri
|string
a|The token introspection endpoint URI.


|interval
|string
a|The refresh interval for caching tokens, in ISO-8601 format. This can be
set to the value "disabled" to disable caching of tokens. When set to 0,
tokens are cached according to the expiry period in them. Otherwise, it
can be set to a value from 1 second to 2147483647 seconds.


|===

[#jwks]
[.api-collapsible-fifth-title]
jwks

[cols=3*,options=header]
|===
|Name
|Type
|Description

|provider_uri
|string
a|The URI on which the JSON Web Key Set (JWKS) are hosted.


|refresh_interval
|string
a|The refresh interval for the JSON Web Key Set (JWKS), in ISO-8601
format. This can be set to a value from 300 seconds to 2147483647 seconds.


|===

[#security_oauth2]

```

```
[.api-collapsible-fifth-title]
security_oauth2

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|application
|string
a|The name of the application using OAuth 2.0. Required for POST
operations.

|audience
|string
a|The OAuth 2.0 Audience.

|client_id
|string
a|The OAuth 2.0 client ID. Required in POST operations for remote
introspection.

|client_secret
|string
a|The OAuth 2.0 client secret. Required in POST operations for remote
introspection.

|hashed_client_secret
|string
a|The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with
the cluster UUID as its HMAC secret key.

|introspection
|link:#introspection[introspection]
a|

|issuer
```

```

|string
a|The OAuth 2.0 Issuer.

|jwks
|link:#jwks[jwks]
a|

|name
|string
a|The configuration name. Required for POST operations.

|outgoing_proxy
|string
a|Outgoing proxy to access external identity providers (IdPs). If not
specified, no proxy is configured.

|remote_user_claim
|string
a|The remote user claim.

|skip_uri_validation
|boolean
a|Indicates whether or not to validate the input URIs. Default value is
false.

|use_local_roles_if_present
|boolean
a|Indicates whether or not to use locally configured roles, if present.
Default value is false.

|use_mutual_tls
|string
a|OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to
disable mutual TLS authentication. Set this value to "required" to enforce
mutual TLS authentication for all access tokens and reject any token that
does not have x5t#S256 property in the cnf section. The default value is
"request" which means mutual TLS authentication is enforced only if the
x5t#S256 property is present in the cnf section of the access token.

|===

```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```
[#returned_error]
```

```
[.api-collapsible-fifth-title]
```

```
returned_error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|arguments
```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

[[ID830940351ee4e1549d2d966b26dd7bce]]

= Create the OAuth 2.0 configuration

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-block]#`/security/authentication/cluster/oauth2/clients`#

Introduced In: 9.14

Creates the OAuth 2.0 configuration.

== Required properties

* `name`

* `application`

* `issuer`

== Optional properties

* `audience`

* `client_id`

* `client_secret`

* `introspection.endpoint_uri`

* `introspection.interval`

* `remote_user_claim`

* `jwks.provider_uri`

* `jwks.refresh_interval`

* `outgoing_proxy`

* `use_local_roles_if_present`

* `skip_uri_validation`

* `use_mutual_tls`

== Related ONTAP commands

* `security oauth2 client create`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_timeout

|integer

|query

|False

a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

* Default value: 1

* Max value: 120

* Min value: 0

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

* Default value:

|===

== Request Body

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|application
|string
a|The name of the application using OAuth 2.0. Required for POST
operations.

|audience
|string
a|The OAuth 2.0 Audience.

|client_id
|string
a|The OAuth 2.0 client ID. Required in POST operations for remote
introspection.

|client_secret
|string
a|The OAuth 2.0 client secret. Required in POST operations for remote
introspection.

|hashed_client_secret
|string
a|The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with
the cluster UUID as its HMAC secret key.

|introspection
|link:#introspection[introspection]
a|

|issuer
|string
a|The OAuth 2.0 Issuer.

```

```

|jwks
|link:#jwks[jwks]
a|

|name
|string
a|The configuration name. Required for POST operations.

|outgoing_proxy
|string
a|Outgoing proxy to access external identity providers (IdPs). If not
specified, no proxy is configured.

|remote_user_claim
|string
a|The remote user claim.

|skip_uri_validation
|boolean
a|Indicates whether or not to validate the input URIs. Default value is
false.

|use_local_roles_if_present
|boolean
a|Indicates whether or not to use locally configured roles, if present.
Default value is false.

|use_mutual_tls
|string
a|OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to
disable mutual TLS authentication. Set this value to "required" to enforce
mutual TLS authentication for all access tokens and reject any token that
does not have x5t#S256 property in the cnf section. The default value is
"request" which means mutual TLS authentication is enforced only if the
x5t#S256 property is present in the cnf section of the access token.

|===

```

.Example request

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application": "http",
  "hashed_client_secret": "string",
  "introspection": {
    "endpoint_uri": "https://examplelab.customer.com/token/introspect",
    "interval": "PT1H"
  },
  "issuer": "https://examplelab.customer.com",
  "jwks": {
    "provider_uri": "https://examplelab.customer.com/pf/JWKS",
    "refresh_interval": "PT2H"
  },
  "name": "auth0",
  "outgoing_proxy": "https://johndoe:secretpass@proxy.example.com:8080",
  "use_mutual_tls": "none"
}
====
```

== Response

Status: 202, Accepted

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|job
|link:#job_link[job_link]
a|

|===

.Example response
[%collapsible%closed]
```

```

=====
[source,json,subs=+macros]
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
=====

=== Headers

[cols=3*,options=header]
|===
//header
|Name
|Description
|Type
//end header

//start row
|Location
|Useful for tracking the resource location
|string
//end row
//end table
|===

== Response

```

Status: 201, Created

```
== Error
```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description

```

| 203817010
| Client ID is required for remote introspection.

| 203817011
| Client secret is required for remote introspection.

| 203817012
| Client ID and client secret required for remote introspection.

| 203817013
| JWKS URI should not be configured for remote introspection.

| 203817014
| JWKS refresh interval should not be specified for remote introspection.

| 203817015
| The token introspection endpoint is required for remote introspection.

| 203817016
| JWKS refresh interval provided without providing JWKS URI.

| 203817017
| Minimum supported value of JWKS refresh interval is 300 seconds.

| 203817018
| Required parameters for either local validation or remote introspection are missing. Provide either the JWKS URI for local validation, or metadata configuration URI or token introspection endpoint with client ID and secret for remote introspection.

| 203817019
| Failed to add new IDP client because number of maximum supported IDP clients is already reached.

| 203817020
| Internal error. Failed to validate provider URI.

| 203817021
| OAuth 2.0 Provider URI validation failed with error.

| 203817022
| OAuth 2.0 Provider JWKS URI validation failed. Received empty response message from the JWKS URI.

| 203817023
| OAuth 2.0 Provider JWKS URI validation failed. No keys were found in response message received from the JWKS URI.

```

| 203817024
| Internal error. Unable to allocate memory for CURL response.

| 203817025
| Maximum value of JWKS refresh interval is 2147483647 seconds.

| 203817033
| OAuth 2.0 Provider Introspection endpoint validation failed. Received
empty response message from the Introspection endpoint.

| 203817034
| OAuth 2.0 Provider Introspection endpoint validation failed. Received
invalid response message for Introspection request.

| 203817042
| Maximum value of introspection interval is 2147483647 seconds.
|===

```

Also see the table of common errors in the
[xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_body\[Response body\]](#) overview section of this documentation.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#returned_error[returned_error]
a|

|===

```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    }
  }
}

```

```

    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```



```

[#introspection]
[.api-collapsible-fifth-title]
introspection

[cols=3*,options=header]
|===
|Name
|Type
|Description

|endpoint_uri
|string
a|The token introspection endpoint URI.

|interval
|string
a|The refresh interval for caching tokens, in ISO-8601 format. This can be
set to the value "disabled" to disable caching of tokens. When set to 0,
tokens are cached according to the expiry period in them. Otherwise, it
can be set to a value from 1 second to 2147483647 seconds.

|===

[#jwks]
[.api-collapsible-fifth-title]
jwks

[cols=3*,options=header]
|===
|Name
|Type
|Description

|provider_uri
|string
a|The URI on which the JSON Web Key Set (JWKS) are hosted.

|refresh_interval
|string
a|The refresh interval for the JSON Web Key Set (JWKS), in ISO-8601
format. This can be set to a value from 300 seconds to 2147483647 seconds.

```

|===

```
[#security_oauth2]
[.api-collapsible-fifth-title]
security_oauth2
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|application
|string
a|The name of the application using OAuth 2.0. Required for POST
operations.
```

```
|audience
|string
a|The OAuth 2.0 Audience.
```

```
|client_id
|string
a|The OAuth 2.0 client ID. Required in POST operations for remote
introspection.
```

```
|client_secret
|string
a|The OAuth 2.0 client secret. Required in POST operations for remote
introspection.
```

```
|hashed_client_secret
|string
a|The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with
the cluster UUID as its HMAC secret key.
```

```
|introspection
|link:#introspection[introspection]
a|
```

```
|issuer
|string
a|The OAuth 2.0 Issuer.
```

```
|jwks
|link:#jwks[jwks]
a|
```

```
|name
|string
a|The configuration name. Required for POST operations.
```

```
|outgoing_proxy
|string
a|Outgoing proxy to access external identity providers (IdPs). If not
specified, no proxy is configured.
```

```
|remote_user_claim
|string
a|The remote user claim.
```

```
|skip_uri_validation
|boolean
a|Indicates whether or not to validate the input URIs. Default value is
false.
```

```
|use_local_roles_if_present
|boolean
a|Indicates whether or not to use locally configured roles, if present.
Default value is false.
```

```
|use_mutual_tls
|string
a|OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to
disable mutual TLS authentication. Set this value to "required" to enforce
mutual TLS authentication for all access tokens and reject any token that
```

does not have x5t#S256 property in the cnf section. The default value is "request" which means mutual TLS authentication is enforced only if the x5t#S256 property is present in the cnf section of the access token.

|===

[#job_link]
[.api-collapsible-fifth-title]
job_link

[cols=3*,options=header]

|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message

```

|string
a|Message argument

|===

[#returned_error]
[.api-collapsible-fifth-title]
returned_error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

```

:leveloffset: -1

<<<

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b) (3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable,

worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at [link:http://www.netapp.com/TM](http://www.netapp.com/TM)^[http://www.netapp.com/TM^] are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.