Client Authentication

Overview

The REST API authentication works as follows:

- The authentication uses HTTPS as the transport for all the Cisco REST API access.
- Clients perform authentication with this service by invoking a POST on this resource with HTTP Basic Auth as the authentication mechanism. The response of this request includes a token-id. Token-ids are short-lived, opaque objects that represents client's successful authentication with the token service.
- Clients then access other APIs by including the token id as a custom HTTP header "X-auth-token". If this token is not present or expired, then API access will return an HTTP status code of "401 Unauthorized"
- Clients can also explicitly invalidate a token by performing a DELETE operation on the token resource.
- The username/password for the HTTPS session should be configured with privilege 15.

Resource Summary for Client Authentication

		HTTP Method			
Resource	**URL (BaseURL)**	**GET**	**POST**	**PUT**	**DELETE**
token-id	/api/v1/auth/token-services	Y	Y	N	N
	/api/v1/auth/token-services/{opaque-token-id}	Y	N	N	Y

Token Service Resource

The token service resource represents the authentication service that allows clients to perform authentication and obtain a token-id.

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

JSON Representation

```
{
  "kind": "collection#auth-token",
  "items: [ { auth-token JSON object }+ ]
}
```

Authenticate and Create a New Token

The initial HTTP request is performed by clients to authenticate and obtain a token so that it can invoke other APIs. The HTTP POST response contains an ‘opaque’ URL to be used for HTTP GET and DELETE requests.

Resource URI

Verb	URI
POST	/api/v1/auth/token-services

Example

JSON Request

```
POST  /api/v1/auth/token-services
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
  "kind": "object#auth-token",
  "token-id": "1ZA23BC",
  "link":http://host/api/auth/token-services/johnDoe,
  "expiry-time": "00:15:00"
}
In subsequent API accesses, the token-id must appear as a custom HTTP header for
successful invocation of APIs.
X-auth-token: {token-id}
```

For example:

```
X-auth-token: "12a23bc"
```

Retrieve Active Tokens

Resource URI

Verb	URI
GET	/api/v1/auth/token-services

Example

JSON Request

```
GET  /api/v1/auth/token-services
X-auth-token: "1za23bc"

Accept: application/json
```

JSON Response

```
403 Access Denied
```

Token Resource

A token represents successful authentication of a client.

History

Release	Modification
IOS XE 3.10	Introduced for the CSR1000V platform
IOS XE 3.14	Introduced for ASR1001-X and ASR1002-X platforms

Properties

Properties	Type	Required for POST and PUT	Description
kind	string	Not applicable	Must be “object#auth-token”
token-id	string	Not applicable	Authentication token that must be included as a custom HTTP header X-auth-token value in all API requests

Properties	Type	Required for POST and PUT	Description
link	string	Not applicable	Token resource URL.
expiry-time	string	Not applicable	Idle period in hh:mm:ss format.

JSON Representation of a Token

```
{
  "kind": "object#auth-token",
  "token-id": "{string}",
  "link":      "{string}",
  "expiry-time": "{string}"
}
```

Retrieve Token Details

Resource URI

Verb	URI
GET	/api/v1/auth/token-services/{opaque-token-id}

Example

JSON Request

```
GET  /api/v1/auth/token-services/johnDoe
X-auth-token: "1za23bc"
Accept: application/json
```

JSON Response

```
200 OK

Content-Type: application/json

{
  "kind": "object#session-token",
  "token-id": "1za23bc"
  "expiry-time": "00:15:00"
}
```

Invalidate a Token

Typically tokens automatically expire after 15 minutes. However, clients can perform explicit invalidation of a token by doing a DELETE on the token resource.

Resource URI

Verb	URI
DELETE	/api/v1/auth/token-services/{opaque-token-id}