

Generating authentication tokens for end-users via the API

The API provides a method to generate an OpenAthens authentication token for a given account, e.g. when you want to have a sign-in form in your own portal.

Generating a new token

Prerequisites

To generate a new token, a client application must

- authenticate to the API using an API key as described in [Authenticating to the API](#). You should use the read-only 'https://login.openathens.net/api/v1/...' address.

Procedure

Perform a POST request to the following URL:

`/api/v1/example.org/account/session`

With the following querystring parameter:

Querystring Parameter	Description
<code>returnUrl</code>	The URL that the user will be returned to after the session has been established. This will usually be a link to a page in the application making the request, e.g. a resource catalogue or library portal.

The request **must** be accompanied with the 'returnUrl' parameter.

Request payload

This should be an `application/vnd.eduserv.iam.user.credential-v1+json` object containing a user identifier and a password

Accounts are identified using one of three unique identifiers and the password

Object field	Description
<code>username</code>	Containing one of either: <ul style="list-style-type: none">• The account username,• The unique email address associated with the account – i.e. the 'uniqueEmailAddress' attribute, if set, or• The persistent user ID (PUID) for the account
<code>password</code>	The account's password

Response payload

The response payload is an `application/vnd.eduserv.iam.auth.transferToken-v1+json` object.

`application/vnd.eduserv.iam.auth.transferToken-v1+json` object

Object field	Description
<code>username</code>	The account username
<code>expiry</code>	The time at which the given token expires
<code>sessionInitiatorUrl</code>	The location to which the user should be redirected to establish the session

Response codes

HTTP Response Code	Description
200	The token was generated
400	The request was invalid

403	Forbidden
404	The account could not be found

The user should be redirected to the URL specified by 'sessionInitiatorUrl'. The format of the URL that is returned may change so calling applications must not alter or infer the structure of this URL in any way.

When the user is passed to the `returnUrl`, it will contain an additional `status` parameter to indicate whether the request was successful. This may optionally be used by the calling application to take action depending on whether the operation was successful or otherwise. Aside from token expiry though, there are almost no reasons why a failure would occur.

Status	Description
Success	The OpenAthens session was established successfully.
TokenExpired	The session initiator token in the request has expired (tokens are valid for 60 seconds after they are issued).
SessionFailure	The OpenAthens system was unable to establish the session (non-specific error).

Example

```
Request:
POST /api/v1/example.org/account/session?returnUrl=<returnUrl> HTTP/1.1
Authorization: OAApiKey <api-key>
Content-Type: application/vnd.eduserv.iam.user.credential-v1+json
{
  "username": "example_username",
  "password": "8d34-ab03-3Pda"
}

Response:
HTTP/1.1 200 OK
Content-Type: application/vnd.eduserv.iam.auth.transferToken-v1+json
{
  "username" : "example_username",
  "expiry" : "2020-08-20T15:48:00Z",
  "sessionInitiatorUrl" : "https://login.openathens.net/account/sso?
token=FGdsghjytj6y54y46J54yrthTR45yersdfhewkjfhwjkhfkhfwjkhfkhewjkhfkhewjefwe",
  "links": [
    {
      "username" : "example_username",
      "href" : "/api/v1/example.org/account/example_account",
      "rel" : "self",
      "type" : "application/vnd.eduserv.iam.account-v1+json",
      "method" : "get",
    }
  ]
}
```

This method involves an additional API call and response, so will be marginally slower for customers who are far from the UK. It has been superseded, but will continue to be supported through at least 2021.

Procedure

Perform a GET request to the following URL:

`/api/v1/example.org/organisation/<id>/account/session`

With the following querystring parameters:

Querystring Parameter	Description
username	Exactly one of these parameters must be included to identify the account.
email	
persistentUID	

returnUrl	The URL that the user will be returned to after the session has been established. This will usually be a link to a page in the application making the request, e.g. a resource catalogue
-----------	--

The request **must** also be accompanied with a 'returnUrl' parameter.

Accounts are identified using one of the following three unique identifiers:

- The OpenAthens account username
- The unique email address associated with the account – i.e. the 'uniqueEmailAddress' attribute, if set.
- The persistent user ID (PUID) for the account.

To generate a token for an individual account based on username perform a GET request to:

```
/api/v1/example.org/organisation/<id>/account/session?username=expuser01&returnUrl=https%3A%2F%2Fexample.org%2Fmy-app
```

To generate a token for an individual account based on email address perform a GET request to:

```
/api/v1/example.org/organisation/<id>/account/session?email=alex@example.org&returnUrl=https%3A%2F%2Fexample.org%2Fmy-app
```

To generate a token for an individual account based on PUID perform a GET request to:

```
/api/v1/example.org/organisation/<id>/account/session?persistentUID=abcd1234%3A456789a&returnUrl=https%3A%2F%2Fexample.org%2Fmy-app
```

Response payload

The response payload is an `application/vnd.eduserv.iam.auth.transferToken-v1+json` object.

application/vnd.eduserv.iam.auth.transferToken-v1+json object

Object field	Description
username	The account username
expiry	The time at which the given token expires
sessionInitiatorUrl	The location to which the user should be redirected to establish the session

Response codes

HTTP Response Code	Description
200	The token was generated
400	The request was invalid
403	Forbidden
404	The account could not be found

The user should be redirected to the URL specified by 'sessionInitiatorUrl'. The format of the URL that is returned may change so calling applications must not alter or infer the structure of this URL in any way.

When the user is passed to the `returnUrl`, it will contain an additional `status` parameter to indicate whether the request was successful. This may optionally be used by the calling application to take action depending on whether the operation was successful or otherwise. Aside from token expiry though, there are almost no reasons why a failure would occur.

Status	Description
Success	The OpenAthens session was established successfully.
TokenExpired	The session initiator token in the request has expired (tokens are valid for 60 seconds after they are issued).
SessionFailure	The OpenAthens system was unable to establish the session (non-specific error).

Example

```
Request:
GET /api/v1/example.org/organisation/123456/account/session?username=<username>&returnUrl=<returnUrl> HTTP/1.1
Authorization: OAApiKey <api-key>
Response:
HTTP/1.1 200 OK
Content-Type: application/vnd.eduserv.iam.auth.transferToken-v1+json
{

  "username" : "example_username",
  "expiry" : "2013-08-20T15:48:00Z",
  "sessionInitiatorUrl" : "https://login.openathens.net/account/sso?
token=FGdsghjytj6y54y46J54yrthTR45yersdfhewkjfhwjkhfhejkhfwjkfhjkwjefwe",
  "links": [
    {
      "username" : "example_username",
      "href" : "/api/v1/example.org/account/example_account",
      "rel" : "self",
      "type" : "application/vnd.eduserv.iam.account-v1+json",
      "method" : "get",
    }
  ]
}
```

See also:

- [API overview](#)
- [Authenticating to the API](#)
- [API entry-point](#)
- [Fetching attribute schemas via the API](#)
- [Fetching organisations via the API](#)
- [Fetching Groups via the API](#)
- [Account management via the API](#)
- [API bulk operations](#)
- [Fetching available service providers via the API](#)
- [Generating authentication tokens for end-users via the API](#)
- [API usage examples](#)