<https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630>

OAuth 2.0 (Client Credentials) as a Token-Based Protocol for API Authentication

* [Overview](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId-479864146)
* [SCIM Protocol](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId-1367367827)
* [Supported HTTP Methods](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId-447417045)
* [Authentication](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId--1152592107)
* [Basic Authentication](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId--2072542889)
* [OAuth 2.0](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId--1185039208)
* [OAuth Client Management Page](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId--2104989990)
* [How To Create An OAuth Client](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId-1270026524)
* [How to get Access Token for OAuth](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId--1010040998)
* [Sample output](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId--1249933410)
* [Access IdentityIQ API](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId-1814982025)
* [Sample Output](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId-2112945191)
* [Additional Resources](https://community.sailpoint.com/t5/IdentityIQ-Wiki/OAuth-2-0-Client-Credentials-as-a-Token-Based-Protocol-for-API/ta-p/77630#toc-hId--704977909)

**Overview**

The IdentityIQ API provides access to the IdentityIQ platform, allowing new opportunities for expanded innovation.

You can use your API to access IdentityIQ API endpoints, which allows to programmatically invoke IdentityIQ API to interact with objects within IdentityIQ.

This document provide insight to use OAuth 2.0 Authentication

SCIM Protocol

SCIM stands for System for Cross-Domain Identity Management, and it is an HTTP-based protocol that makes managing identities in

multi-domain scenarios easier to support through a standardized RESTful API service. It provides a platform neutral schema and extension

model for representing users, groups and other resource types in JSON format

Supported HTTP Methods

* GET
* POST
* PUT
* DELETE

Authentication

Basic Authentication

Beginning in IdentityIQ version 7.0, Patch 2, Basic Authentication is used to allow access to the API. Basic authentication is a simple

technique for enforcing access controls to API resources because it doesn’t require session IDs, cookies, or login pages but instead uses

standard fields in the HTTP header. For more information on Basic authentication, please see <https://tools.ietf.org/html/rfc1945#section-11>

and <https://www.ietf.org/rfc/rfc2617.txt>. Support for Basic Authentication will continue to exist in future releases.

OAuth 2.0

OAuth 2.0 Authentication will be supported in IdentityIQ Version 7.1. Versions prior to 7.1 only support Basic Authentication.

OAuth Client Management Page

The OAuth Client Management page has the following tabs and options:

• OAuth Client Management tab — displays a list of the current OAuth clients.

     - Create Button — creates an OAuth client that has a proxy user with an associated secret.

     - Secret Details icon — displays the secret for the an OAuth client.

     - Actions icons — Edit, Delete, Regenerate Secret

• General Settings tab

     - Access Token Expiration In Seconds

How To Create An OAuth Client

     1.From the top menu, navigate to the Gear icon > Global Settings > API Authentication.

     2.On the OAuth Client Management tab, click Create.

     3.In the OAuth Client dialog enter a unique name for Client Name and then enter a user name or select a user from the drop-down list for the Proxy User.

     4.Click Save to save your new OAuth client.

          After your create an OAuth client, you can use it with the associated secret to log in and access the token for that proxy user

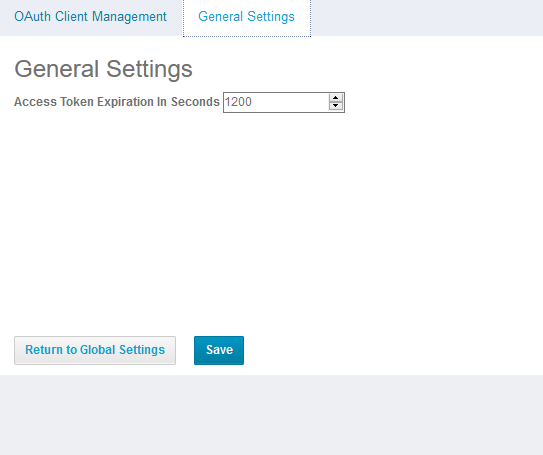
How to get Access Token for OAuth

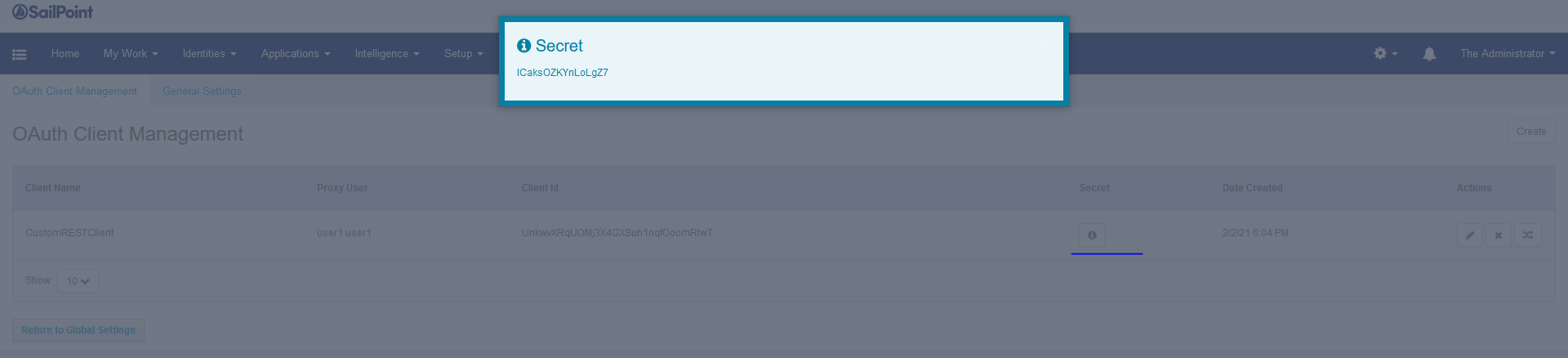
When we are enabling OAuth authentication, we should get access token before invoking IdenttiyIQ API.

we should use the following details to get access token from IdentityIQ,

* client\_id - will get client id from OAuth client management
* client\_secret - will get client id from OAuth client management
* grant\_type (client\_credentials)
* Token URL - "<http://localhost:8080/identityiq/oauth2/token>"







## User Rights:

