NetIQ Secure API Manager 2.0 Developers Guide for Using the APIs

Technical Reference

March 2021

NetIQ Secure API Manager hosts APIs in a secure environment. Secure API Manager secures access to the APIs through OAuth 2 tokens and NetIQ Access Manager roles and scopes. To be able to use and consume the APIs from Secure API Manager in applications, services, or devices you must know how to properly call the APIs.

This article describes how Secure API Manager protects the APIs and how to properly consume the APIs.

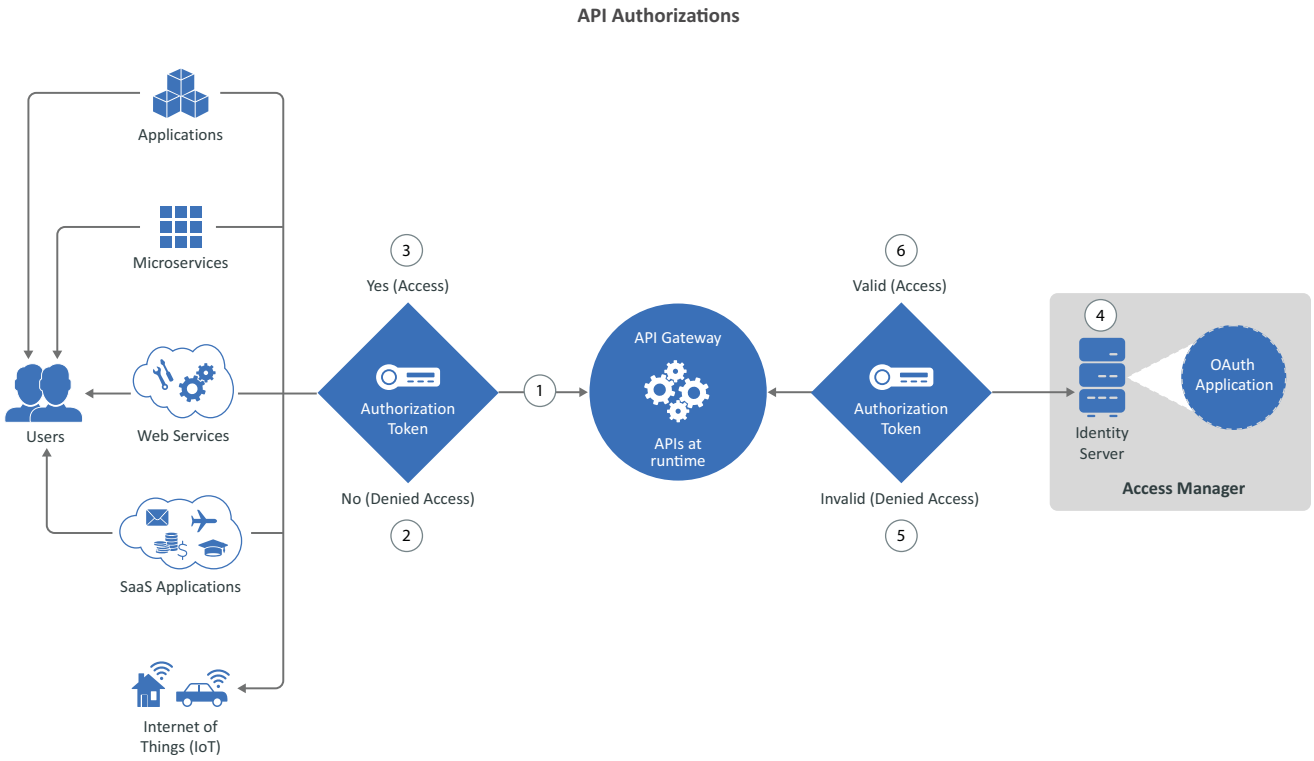
- "How Secure API Manager Authorizes the APIs" on page 1
- "Obtain an OAuth Token to Make API Calls" on page 2

How Secure API Manager Authorizes the APIs

Secure API Manager controls access to APIs through OAuth authorizations. When you configure Secure API Manager, it automatically creates an OAuth 2 application for you in Access Manager. Secure API Manager uses the authorizations tokens from this OAuth 2 application to secure access to the APIs. When an API developer

creates an API in the Publisher, the developer adds the authorization token to the API from this OAuth 2 application. The following graphic shows the flow of the API authorization from the application, service or item through the API Gateway to the Access Manager Identity Server.

Figure 1 *How Secure API Manager Authorizes APIs*



1. When an application, service, or item calls an API, the call accesses the API stored on the API Gateway. The API Gateway contains the APIs in a run-time environment.
2. The API Gateway checks to see if the call for the API contains an OAuth token. If it does not, the API Gateway rejects the call and the application, service, or item receives a message stating the API is not available.
3. If the call for the API does contain an OAuth token, the API Gateway sends the call to the Identity Server.
4. The Identity Server checks the OAuth application to see if the token is valid.
5. If the token is not valid, the Identity Server sends that information to the API Gateway and the API Gateway rejects the call. The application, service, or item receives a message stating that the API is not available.
6. If the token is valid, the Identity Server sends that information to the API Gateway. The API Gateway then allows the call for the API to execute and the application, service, or item receives the additional functionality from the API.

Obtain an OAuth Token to Make API Calls

After you have subscribed to an API, you can use two different OAuth methods to make API calls through Secure API Manager. The endpoints are defined in the OAuth 2.0 RFC under Protocol Endpoints.

- "Authorization Endpoint" on page 3
- "Token Endpoint" on page 3

Authorization Endpoint

The authorization endpoint employs Access Manager as the owner of the user's credentials and the handler of the authentication process. The advantage to using this method is that the client implementation never obtains the user's credentials. It also allows Access Manager to execute multi-factor authentications. This is the preferred method.

To invoke the authorization profile, create an authorized endpoint request as described in the *Access Manager 5.0 OAuth Application Developer Guide*. An additional step that is specific to Secure API Manager is to include the scope `APIManagerScope` in the list of scopes in the request.

Token Endpoint

The token endpoint profile allows a client that has the user's credentials to obtain an OAuth2 token in a single request. To invoke this endpoint, the client must own the client's username and password. Many client implementations do not want to protect the user's credentials (or ever have them go to the client) so this method is generally not preferred.

To invoke the token profile, create a token endpoint request as defined in the *Access Manager 5.0 OAuth Application Developer Guide*. You must perform an additional step that is specific to Secure API Manager. You must include the scope `APIManagerScope` in the list of scopes in the request. For example:

```
grant_type=password&client_id=557c9074-6a09-4f1a-83a6-
0d3b442e1cc0&client_secret=he3Mmy3IGgL9dxhufNHo312DQqTJYI8mB6GHA&username=fred&pa
ssword=test0123&scope=APIManagerScope
```