Esquema de Seguridad SIGT

Prerrequisitos:

1. Haber realizado la solicitud y estar aprobada.

Con el correo electrónico del representante legal que realizo la solicitud o el correo electrónico corporativo, pueden hacer las solicitudes para generar el token de autorización a continuación se relacionan los datos de configuración para la ambiente calidad y productivo.

Método: POST

1. **Endpoint**

Calidad: https://am-aeu-mt-qas-shrd.azure-api.net/commons/api/User/Authentication

Producción: https://am-aeu-mt-prd-shrd.azure-api.net/commons/api/User/Authentication

2. **ClientId**

Calidad: 5e829a0c-9ed2-4360-8d59-44e6315cbad1

Producción: 287c76a7-f17a-4730-b2a3-3b1d0436f11b

3. **TenantId**

Calidad: 9c0fcd43-c3d6-4dcb-b602-2b16ffe332c6

Producción: 9c0fcd43-c3d6-4dcb-b602-2b16ffe332c6

Datos de la petición

1. **Encabezado la petición**

Ambiente	Variable	Value
Calidad	Ocp-Apim-Subscription-Key	f24f3646636a4c0d978e2951f3066864
Producción	Ocp-Apim-Subscription-Key	8120b364ad754df8927233b2c2840c29

2. **Cuerpo de la petición**

content type json
username: correo electrónico corporativo o del representante legal con el que ingreso o fue invitado por la plataforma SIGT.
password: contraseña del usuario con el que ingreso a la plataforma SIGT.
clientId: este valor es una constante y no cambia.

```
{
  "username": "user@dominio ",
  "password": "test",
  "clientId": "5e829a0c-9ed2-4360-8d59-44e6315cbad1"
}
```

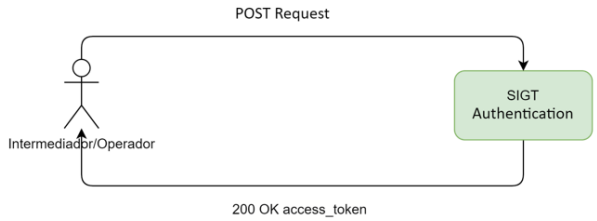


Ilustración 1. Generación del token de autorización.

Ejemplo de la Petición en la herramienta postman

A continuación, se relaciona un ejemplo de cómo se debe enviar la petición.

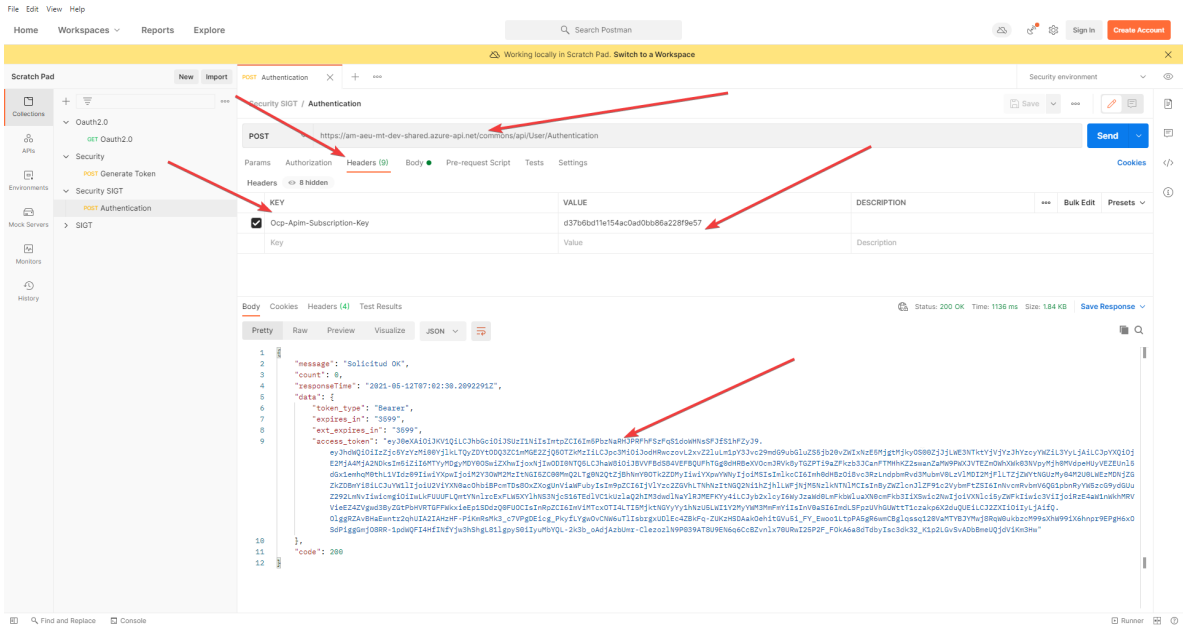


Ilustración 2: Petición Postman

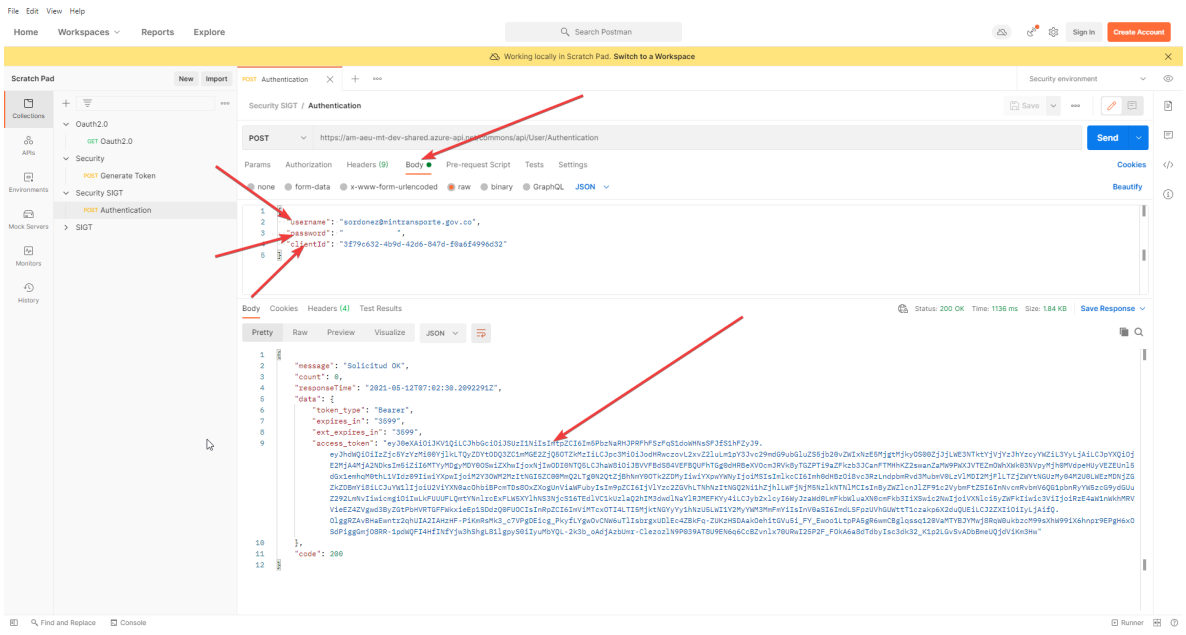


Ilustración 3: Cuerpo de la petición

Verificación de TOKEN:

Los actores deben revisar que el token que llega en cada petición se encuentre activo, y para ello se hace de la siguiente manera.


```
  "iss": "https://login.microsoftonline.com/9c0fcd43-
c3d6-4dcb-b602-2b16ffe332c6/v2.0",
  "iat": 1664270427,
  "nbf": 1664270427,
  "exp": 1664274429,
  "aio":
"AVQAq/8TAAAA/QrT1/3USgLIlJ1H20U8JVx2PiG6X65CMHS6pxUkXp
Rgij1URivg/nhk28JHlh+lSWs+WfXug+YndRkWOV7iWuIvA+4XMxro3
MsjMEjnNvc=",
  "azp": "5e829a0c-9ed2-4360-8d59-44e6315cbad1",
  "azpacr": "0",
  "idp": "https://sts.windows.net/5e02621e-6cef-4e33-
83e4-a303cdfdd0fb/",
  "name": "Cesar Augusto Gomez Perilla",
  "oid": "ffb151b1-d788-43a4-926e-daedaed4fdb9",
  "preferred_username": "cgomezp@mintransporte.gov.co",
  "rh": "0.AR4AQ80PnNbDy022AisW_-
Myxgyagl7SnmBDjVlE5jFcutEeAE8.",
  "scp": "User.read",
  "sub": "1BlQ2gK-i-D3-p3pLMQNyhyzCQsq582nXxM4cmvdEEc",
  "tid": "9c0fcd43-c3d6-4dcb-b602-2b16ffe332c6",
  "uti": "IzftPbbrukWoWdF09zgPAA",
  "ver": "2.0"
}
```


El atributo exp o Tiempo de expiración, es la fecha que sirve para verificar si el JWT está vencido y obligar al usuario a volver a autenticarse.

Valida Habilitación: Endpoint que se encarga se validar si un operador/intermediador se encuentra habilitado ante el SIGT.

Método: GET

Calidad: https://am-aeu-mt-qas-shrd.azure-api.net/base/api/Habilitacion/ValidaHabilitacion/{idUser}

Produccion: https://am-aeu-mt-prd-shrd.azure-api.net/base/api/Habilitacion/ValidaHabilitacion/{idUser}

Header

Ambiente	Variable	Value
Calidad	Ocp-Apim-Subscription-Key	f24f3646636a4c0d978e2951f3066864
Producción	Ocp-Apim-Subscription-Key	8120b364ad754df8927233b2c2840c29

Param: idUser


```
{
  "aud": "287c76a7-f17a-4730-b2a3-3b1d0436f11b",
  "iss": "https://login.microsoftonline.com/9c0fcd43-
c3d6-4dcb-b602-2b16ffe332c6/v2.0",
  "iat": 1637702222,
  "nbf": 1637702222,
  "exp": 1637707185,
  "aio":
"AZQAa/8TAAAArWFVA8g3im3zg+gSOYu1A8zAK0ZAQ4HurG0sQXN8EU
Hm2XHIiMQAjXuguV1zWrDheukaeokLWc1KtPn3JjW6utS1GAVZhISSL
BAGNEoCQF4h1Hai7xPWGly9m1ChLvwANlEL8PqA0UO3hDzB6mqgHPZr
5bw95YuPYY+t7QGVQUBt+WCxwQuOO5cZo+uP8cdV",
  "azp": "287c76a7-f17a-4730-b2a3-3b1d0436f11b",
  "azpacr": "0",
  "idp": "https://sts.windows.net/5e02621e-
6cef-4e33-83e4-a303cdfdd0fb/",
  "name":
  "oid": "e3c9b6e9-8a7e-4ed0-864e-f0f8ca61025b",
  "preferred_username":
"sordonez@mintransporte.gov.co",
  "rh": "0.AR4AQ80PnNbDy022AisW_-
Myxqd2fCh68TBHsqM7HQQ28RseAJc.",
  "scp": "User.read",
  "sub": "GaXA9kFINxzoq736jfBjFsPJs0PjCYCxd8CTuUZoTNw",
  "tid": "9c0fcd43-c3d6-4dcb-b602-2b16ffe332c6",
  "uti": "WWvDQVeWYUmaK2kARptzAQ",
  "ver": "2.0"
}
```


El parámetro idUser corresponde al oid, como se aprecia en la imagen.

Respuesta: si, se encuentra habilitado ante el SIGT la respuesta es true, si no es false.

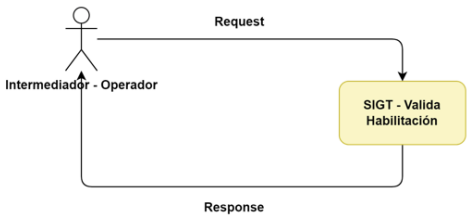


Ilustración 4. SIGT Intermediador y Operador

El formato de la respuesta de la petición Validación es:

```
{
    "message": "Solicitud OK",
    "count": 0,
    "responseTime": "2022-01-21T14:27:55.647",
    "data": {
        "tipoActor": "sigt",
        "estado": true
    },
    "code": 200
}
```

```
{
    "message": "No se encuentra habilitado en el sistema",
    "count": 0,
    "responseTime": "2022-01-21T14:28:16.447",
    "data": {
        "tipoActor": "",
        "estado": false
    },
    "code": 400
}
```


tipoActor: tendra 3 tipos de respuesta[“sigt”, “int”, “op”]

estado: si el Oid es valido devuelve un **true** de lo contrario es **false**

Nota: Se debe tener en cuenta que el IntermediadorRobot y OperadorRobot genera su propio token y así mismo se debe validar que provenga de una fuente confiable.

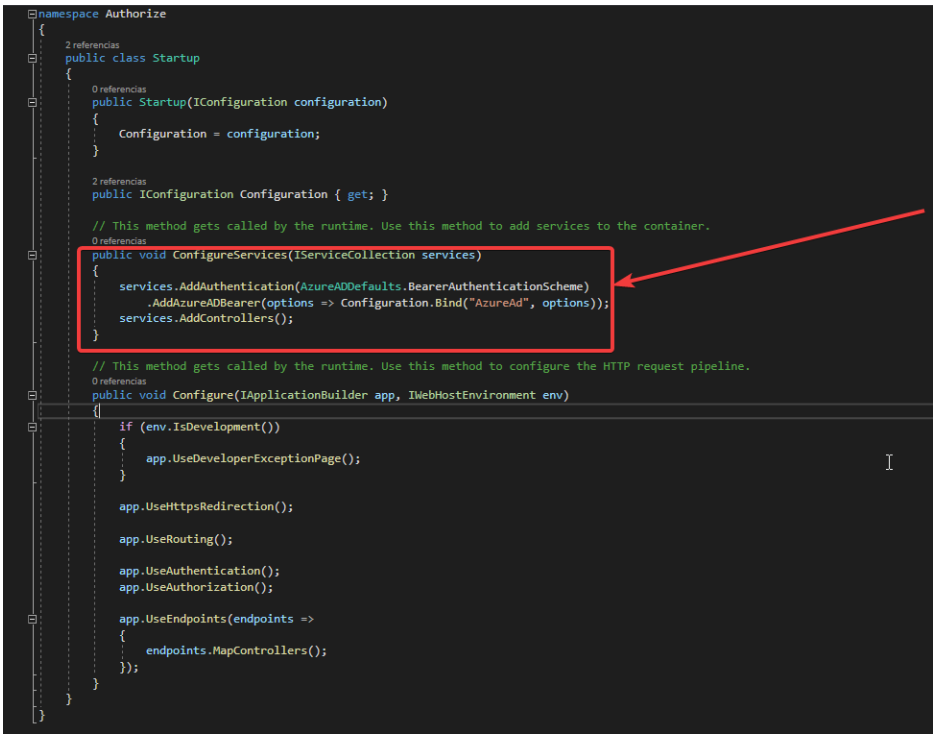
Ejemplo de Autorización

A continuación, se relaciona un archivo de configuración con los valores de las variables.


```
Esquema: https://json.schemastore.org/appsettings.json
{
  "AzureAd": {
    "Instance": "https://login.microsoftonline.com/",
    "TenantId": "eb171928-2929-4f2c-a759-b5cc2ac72afb",
    "ClientId": "3f79c632-4b9d-42d6-847d-f0a6f4996d32",
    "CallbackPath": "/signin-oidc",
    "SignedOutCallbackPath": "/signout-callback-oidc"
  },
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "AllowedHosts": "*"
}
```


Ilustración 5: Configuración de Valores

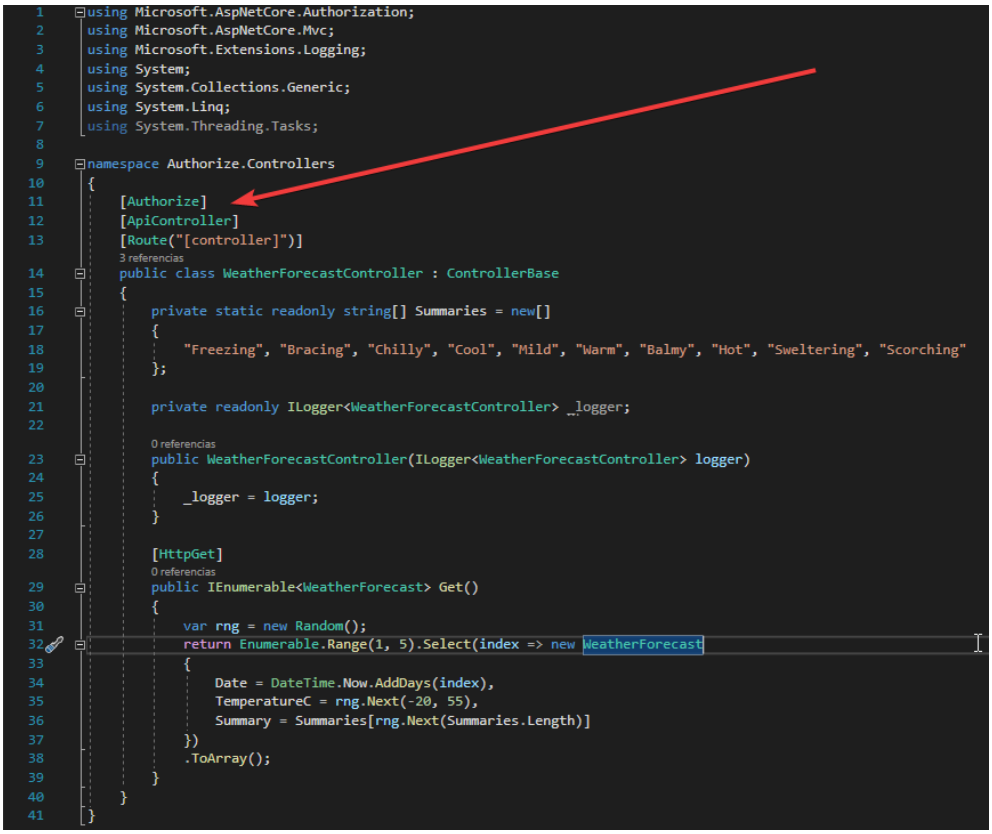
Clase Startup, donde se realiza la configuración de la autorización de las Apis.



```
namespace Authorize
{
    2 referencias
    public class Startup
    {
        0 referencias
        public Startup(IConfiguration configuration)
        {
            Configuration = configuration;
        }

        2 referencias
        public IConfiguration Configuration { get; }

        // This method gets called by the runtime. Use this method to add services to the container.
        0 referencias
        public void ConfigureServices(IServiceCollection services)
        {
            services.AddAuthentication(AzureADDefaults.BearerAuthenticationScheme)
                .AddAzureADBearer(options => Configuration.Bind("AzureAd", options));
            services.AddControllers();
        }

        // This method gets called by the runtime. Use this method to configure the HTTP request pipeline.
        0 referencias
        public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
        {
            if (env.IsDevelopment())
            {
                app.UseDeveloperExceptionPage();
            }

            app.UseHttpsRedirection();

            app.UseRouting();

            app.UseAuthentication();
            app.UseAuthorization();

            app.UseEndpoints(endpoints =>
            {
                endpoints.MapControllers();
            });
        }
    }
}
```

Ilustración 6: Configuración Autorización

Decorado en el controlador con el atributo [**Autorize**].



```
using Microsoft.AspNetCore.Authorization;
using Microsoft.AspNetCore.Mvc;
using Microsoft.Extensions.Logging;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Threading.Tasks;

namespace Authorize.Controllers
{
    [Authorize]
    [ApiController]
    [Route("[controller]")]
    3 referencias
    public class WeatherForecastController : ControllerBase
    {
        private static readonly string[] Summaries = new[]
        {
            "Freezing", "Bracing", "Chilly", "Cool", "Mild", "Warm", "Balmy", "Hot", "Sweltering", "Scorching"
        };

        private readonly ILogger<WeatherForecastController> _logger;

        0 referencias
        public WeatherForecastController(ILogger<WeatherForecastController> logger)
        {
            _logger = logger;
        }

        [HttpGet]
        0 referencias
        public IEnumerable<WeatherForecast> Get()
        {
            var rng = new Random();
            return Enumerable.Range(1, 5).Select(index => new WeatherForecast
            {
                Date = DateTime.Now.AddDays(index),
                TemperatureC = rng.Next(-20, 55),
                Summary = Summaries[rng.Next(Summaries.Length)]
            })
            .ToArray();
        }
    }
}
```

Ilustración 7: Decorado en el controlador

Recursos base documental para la autorización de la petición:

Adición del inicio de sesión en Microsoft a una aplicación web ASP.NET
https://docs.microsoft.com/es-es/azure/active-directory/develop/tutorial-v2-asp-webapp

Adición de inicio de sesión con Microsoft a una aplicación web de Java
https://registeredapps.hosting.portal.azure.net/registeredapps/Content/1.0.01655867/Quickstarts/es/JavaQuickstartPage.html?clientOptimizations=undefined&l=es.es-es&trustedAuthority=https%3A%2F%2Fportal.azure.com&shellVersion=undefined#how-the-sample-works

Adición del inicio de sesión con Microsoft a una aplicación web de Python
https://registeredapps.hosting.portal.azure.net/registeredapps/Content/1.0.01655867/Quickstarts/es/PythonQuickstartPage.html?clientOptimizations=undefined&l=es.es-es&trustedAuthority=https%3A%2F%2Fportal.azure.com&shellVersion=undefined#how-the-sample-works